Maritime cyber lab 2026

From Risk to Resilience

Venue: UN House, Brussels

Proposed Date: 27 – 28 May 2026

1. Background

1. Background

Maritime transport underpins over 80 % of global trade and constitutes a critical component of international economic stability, energy supply, and global supply chains. Ports, shipping companies, offshore installations, and maritime coordination centres are undergoing rapid digital transformation, integrating operational technology (OT), information technology (IT), satellite communications, automated logistics platforms, and interconnected supply-chain systems. While these developments have improved efficiency and connectivity, they have also increased exposure to cyber risks affecting critical maritime infrastructure.

According to the European Union Agency for Cybersecurity (ENISA), the transport sector—including maritime transport and port infrastructure—has experienced a steady increase in cybersecurity incidents in recent years, with ransomware, system intrusion, and data breaches among the most frequently observed attack types. Cyber incidents affecting maritime infrastructure can disrupt port operations, delay cargo handling, compromise operational and safety systems, and generate cascading economic and security impacts across national and international supply chains.

Recognising these risks, the International Maritime Organization (IMO) has formally integrated cyber risk management into maritime safety requirements, including through resolution MSC.428(98), which requires shipping companies to address cyber risks within their safety management systems. At the same time, governments and regional organisations, including the European Union, have strengthened regulatory frameworks to enhance the resilience of critical infrastructure and improve incident prevention, preparedness, and response capabilities.

Despite these advances, maritime cybersecurity remains a shared responsibility involving public authorities, port operators, shipping companies, infrastructure providers, and technology stakeholders. Opportunities for structured dialogue and practical exchange across institutional and sectoral boundaries remain limited, particularly in a rapidly evolving threat environment and regulatory landscape.

Against this backdrop, and leveraging Brussels' role as a global hub for maritime governance and cybersecurity policy, UNITAR is convening the Maritime Cyber Lab as an interactive, practitioner-focused exchange platform. The Lab will bring together public authorities, international organisations, industry representatives, and technical experts to share experiences, discuss emerging risks, and exchange practical approaches to maritime cybersecurity.

Through moderated discussions and collaborative working sessions, participants will reflect on operational challenges, lessons learned, and priority needs, and explore potential avenues to strengthen maritime cyber resilience. The Lab aims to foster mutual learning, strengthen professional networks, and support informed dialogue in alignment with participants' respective mandates and international and regional policy frameworks.

2. Objective of the Maritime Cyber Lab

The Maritime Cyber Lab 2026 will serve as an interactive practitioner-focused exchange and co-creation platform designed to bridge policy dialogue and operational practice. Over two structured working days, the Lab will bring together representatives from governments, port authorities, industry, international organisations, insurers, financial institutions, and technology partners to exchange experiences, discuss emerging maritime cyber risks, and explore practical approaches to strengthening cyber resilience in ports and maritime supply chains.

Rather than functioning as a traditional conference, the Lab is structured as a facilitated working environment. Through expert exchanges, incident reflections, governance discussions, and moderated breakout sessions, participants will share operational perspectives, identify common challenges, and explore practical and scalable approaches across the maritime ecosystem.

Specifically, the Lab aims to:

- Facilitate exchange on systemic maritime cyber risks affecting ports, vessels, and interconnected supply chains, contributing to a shared understanding of priority risk areas.

- Reflect on operational experiences and incident examples to identify practical lessons learned and common challenges across regions and sectors.

- Discuss governance and regulatory perspectives, including roles of port and flag states, regulatory authorities, operators, and insurers, and explore how existing frameworks can support operational resilience.

- Identify priority capacity development needs related to training, institutional coordination, incident preparedness, and technical resilience, informing future cooperation and capacity-building efforts.

- Exchange good practices and practical approaches, including training models, public-private cooperation mechanisms, and operational coordination formats.

- Explore potential areas for continued dialogue, cooperation, and partnership, including possible follow-up activities, pilot initiatives, or knowledge-sharing platforms.

The overall objective of the Maritime Cyber Lab is to foster mutual learning, strengthen professional networks, and support practical and sustainable approaches to maritime cyber resilience, taking into account the diverse operational realities and capacities of maritime stakeholders globally.

3. Programme Design and Agenda

The Maritime Cyber Lab 2026 is designed as a two-day interactive working process structured around expert exchange, collaborative reflection, and practical exploration of maritime cyber resilience approaches.

Day 1 focuses on shared situational awareness and system perspectives through expert inputs, selected incident reflections, governance discussions, and participatory exercises. These sessions will enable participants to exchange experiences, identify common cyber risk areas, and highlight priority challenges related to training, technology, governance coordination, and incident response.

Day 2 shifts toward operational perspectives and cooperation mechanisms, including discussions on incident reporting practices, information-sharing approaches, cross-border coordination, and crisis preparedness. Facilitated breakout sessions will provide space for participants to exchange practical approaches, explore cooperation opportunities, and identify areas for continued dialogue, capacity development, or pilot initiatives.

The Lab will conclude with a summary of key insights and potential areas for follow-up cooperation, informing future dialogue and capacity-building efforts in support of maritime cyber resilience.

4. Participants

The Maritime Cyber Lab will bring together a diverse group of senior practitioners and decision-makers representing key dimensions of maritime cybersecurity, including:

- **Public sector:** Maritime administrations, port authorities, transport and security authorities, and relevant national and European cybersecurity and regulatory bodies.

- **Private sector:** Terminal operators, shipping companies, logistics providers, port infrastructure operators, insurers, classification societies, and financial institutions supporting maritime and port operations.

- **International and regional organisations:** International Maritime Organization (IMO), United Nations entities, European Union institutions, and other relevant international partners.

- **Industry associations and professional organisations:** Including organisations such as the International Association of Ports and Harbors (IAPH), the European Community Shipowners' Associations (ECSA), the International Chamber of Shipping (ICS), and related maritime industry bodies.

- **Technical and operational stakeholders:** Maritime security professionals, infrastructure managers, and cybersecurity practitioners involved in protecting maritime and port systems.

5. Expected Outcomes

- A shared overview of priority capacity development needs related to training, governance coordination, incident preparedness, and technical resilience.

- Exchange of operational lessons and good practices supporting practical and resilience-focused maritime cybersecurity approaches.

- Strengthened mutual understanding of cooperation mechanisms, including incident reporting, information sharing, and coordination practices.

- Identification of potential priority areas and partnership opportunities informing future dialogue and capacity-building initiatives.

- Reinforced professional networks and a collaborative foundation for continued engagement.

6. Strategic Impact

By facilitating structured exchange and practitioner-focused dialogue, the Maritime Cyber Lab aims to support practical progress beyond policy discussion. It will:

- Strengthen alignment between cybersecurity policy frameworks and operational realities across the maritime sector.

- Support maritime stakeholders in identifying practical approaches to strengthening cyber resilience of port, vessel, and logistics infrastructure.

- Promote resilience-focused cybersecurity practices through the exchange of operational experiences and good practices.

- Contribute to improved awareness of systemic cyber risks affecting interconnected maritime supply chains.

- Support broader international and regional efforts to strengthen the resilience of critical maritime infrastructure.

7. Policy and Strategic Alignment

The Maritime Cyber Lab is aligned with key international and regional policy frameworks addressing cybersecurity and the resilience of critical maritime infrastructure. At the global level, this includes relevant United Nations processes, such as United Nations General Assembly resolutions, the UN Open-Ended Working Group, and the 2024 United Nations Convention against Cybercrime. It also reflects the International Maritime Organization’s guidance on maritime cyber risk management, including MSC-FAL.1/Circ.3 Rev.3 and resolution MSC.428(98).

At the regional level, the Lab is consistent with European Union frameworks including the NIS2 Directive, the Critical Entities Resilience Directive, the Cyber Resilience Act, and the Cyber Solidarity Act.

The Lab further reflects internationally recognised cybersecurity standards and best practices, including ISO/IEC 27001:2022, IEC/ISA 62443, and the NIST Cybersecurity Framework 2.0, supporting dialogue aligned with international policy and operational practice.