Unitar Online Catalogue

[Online Attendance] Maritime Cyber Lab: From Risk to Resilience - 2026 Edition

Peace

Deadline: 28 May 2026

Type:	Conference
Location:	Brussels, Belgium
Date:	27 May 2026 to 28 May 2026
Duration:	2 Days
Programme Area:	Peacekeeping
Website:	https://unitar.org/sustainable-development-goals/peace
Price:	$0.00
Event Focal Point Email:	Carolina.martinho@unitar.org

BACKGROUND

The United Nations Institute for Training and Research (UNITAR) is pleased to convene the 2026 edition of the **Maritime Cyber Lab: From Risk to Resilience**, an interactive two-day platform designed for practitioners and decision-makers working across maritime transport, cybersecurity, policy, and critical infrastructure resilience.

Maritime transport underpins more than 80% of global trade and is undergoing a profound digital transformation. Ports, shipping companies, offshore installations, and maritime coordination centres are increasingly reliant on interconnected operational and information technology (OT–IT) systems, satellite communications, automated logistics platforms, and digital port community systems. While these developments significantly enhance efficiency, transparency, and connectivity, they also introduce new and complex vulnerabilities across the maritime domain.

In recent years, the maritime sector has experienced a steady increase in cyber incidents, including ransomware attacks, system intrusions, and data breaches affecting ports, vessels, and logistics chains. Such incidents can disrupt port operations, compromise safety-critical systems, delay cargo flows, and generate cascading economic impacts across global supply chains. As maritime infrastructure becomes more interconnected, vulnerabilities in one node can have far-reaching systemic consequences.

In response, international and regional actors, including the International Maritime Organization (IMO), the European Union, and national authorities, have strengthened regulatory frameworks and guidance to enhance the cyber resilience of maritime infrastructure. These include measures aimed at improving risk management, incident prevention, preparedness, and coordinated response.

Despite this progress, maritime cybersecurity remains a **shared and evolving challenge** that cuts across jurisdictions, sectors, and institutional mandates. Opportunities for structured, cross-sectoral dialogue and practical exchange remain limited, particularly between policy-makers, operational actors, and private-sector stakeholders.

The Maritime Cyber Lab seeks to address this gap by providing a **neutral, practitioner-oriented platform** that brings together public authorities, international organisations, industry representatives, and technical experts. Through facilitated dialogue and collaborative working sessions, participants will explore emerging risks, reflect on operational challenges and lessons learned, and identify priority areas for strengthening maritime cyber resilience.

The Lab aims to contribute to **enhanced cooperation, informed decision-making, and more resilient maritime systems**, supporting both regional and global efforts to safeguard critical maritime infrastructure and international trade.

EVENT OBJECTIVES

The overall objective of the Maritime Cyber Lab is to provide a **practitioner-focused exchange and co-creation platform** that bridges policy dialogue and operational practice.

Specifically, the Lab aims to:

- Facilitate structured exchange on systemic maritime cyber risks affecting ports, vessels, and interconnected supply chains
- Promote a shared understanding of emerging threat patterns, vulnerabilities, and risk dynamics across the maritime ecosystem
- Reflect on operational experiences and real-world incidents to identify practical lessons learned and common challenges
- Examine governance and regulatory perspectives, including roles and responsibilities across public and private actors
- Identify priority capacity-development needs related to training, institutional coordination, incident preparedness, and technical resilience
- Exchange good practices and practical approaches, including training models, public–private cooperation mechanisms, and operational coordination formats
- Explore opportunities for continued dialogue, follow-up initiatives, and knowledge-sharing platforms
- Strengthen professional networks and foster mutual learning across regions and sectors

METHODOLOGY

The Maritime Cyber Lab is grounded in UNITAR's commitment to **practical, evidence-based learning and capacity development**. The Lab combines expert input, facilitated dialogue, and collaborative working formats to connect policy frameworks with operational realities across the maritime domain.

The two-day programme is structured around interactive methodologies that encourage active participation and peer exchange. Sessions will include expert briefings, incident reflections, governance discussions, and moderated breakout groups. These formats allow participants to analyse real-world cases, compare operational practices, and identify shared challenges related to technology, coordination, and preparedness.

Particular emphasis is placed on bridging the gap between **strategic policy discussions and operational implementation**, ensuring that insights generated during the Lab are relevant, actionable, and grounded in real-world practice.

The Lab is aligned with key international and regional frameworks, including the IMO's guidance on maritime cyber risk management, relevant United Nations processes, and European Union regulatory initiatives (such as the NIS2 Directive and the Critical Entities Resilience Directive), as well as recognised cybersecurity standards and best practices.

TARGETED AUDIENCE

The Maritime Cyber Lab brings together a diverse and high-level group of stakeholders from across the maritime and cybersecurity ecosystem, including:

Public sector: Maritime administrations, port authorities, transport and security authorities, and national and European cybersecurity bodies

Private sector: Terminal operators, shipping companies, logistics providers, port infrastructure operators, insurers, classification societies, and financial institutions

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

Industry associations and professional organisations: including the International Association of Ports and Harbors (IAPH), the European Community Shipowners' Associations (ECSA), the International Chamber of Shipping (ICS), and related maritime bodies

Technical and operational stakeholders: Maritime security professionals, infrastructure managers, and cybersecurity practitioners

ADDITIONAL INFORMATION

- Online participation will be registered automatically and will be hosted via Zoom.

- Participation is free of charge. Attendance is possible either in-person in Brussels or online.