Enhancing Maritime Cybersecurity ECSF Role Alignment

COLUMBIA SHIPMANAGEMENT

CYBERGUARD
AI-POWERED DEFENSE

Engaging EU Projects using ECSF

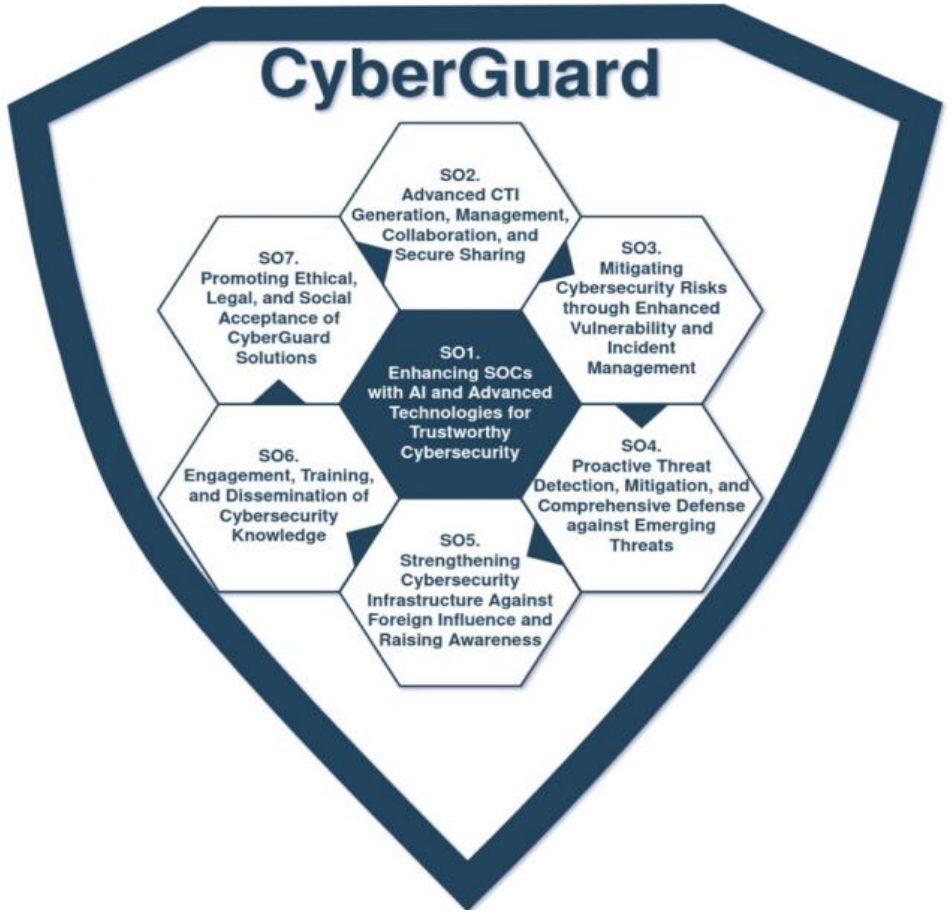
November 2025, Brussels

MARIOS IOANNOU
GROUP BISO
COLUMBIA GROUP

What is CyberGuard?

CYBERGUARD is an EU-funded initiative developing an AI-enhanced SOC platform to strengthen cyber resilience across critical sectors, including maritime. It combines AI, CTI, penetration testing, and incident-response automation to support NIS2-aligned operations.

- **SO1:** Enhance SOCs with AI and advanced cybersecurity technologies
- **SO2:** Enable advanced CTI generation, management, and secure sharing
- **SO3:** Improve vulnerability and incident management capabilities
- **SO4:** Provide proactive threat detection and defense against emerging threats
- **SO5:** Strengthen cybersecurity infrastructure and resilience
- **SO6:** Deliver training, engagement, and knowledge dissemination
- **SO7:** Ensure ethical, legal, and societal acceptance of CYBERGUARD solutions



Co-funded by the European Union

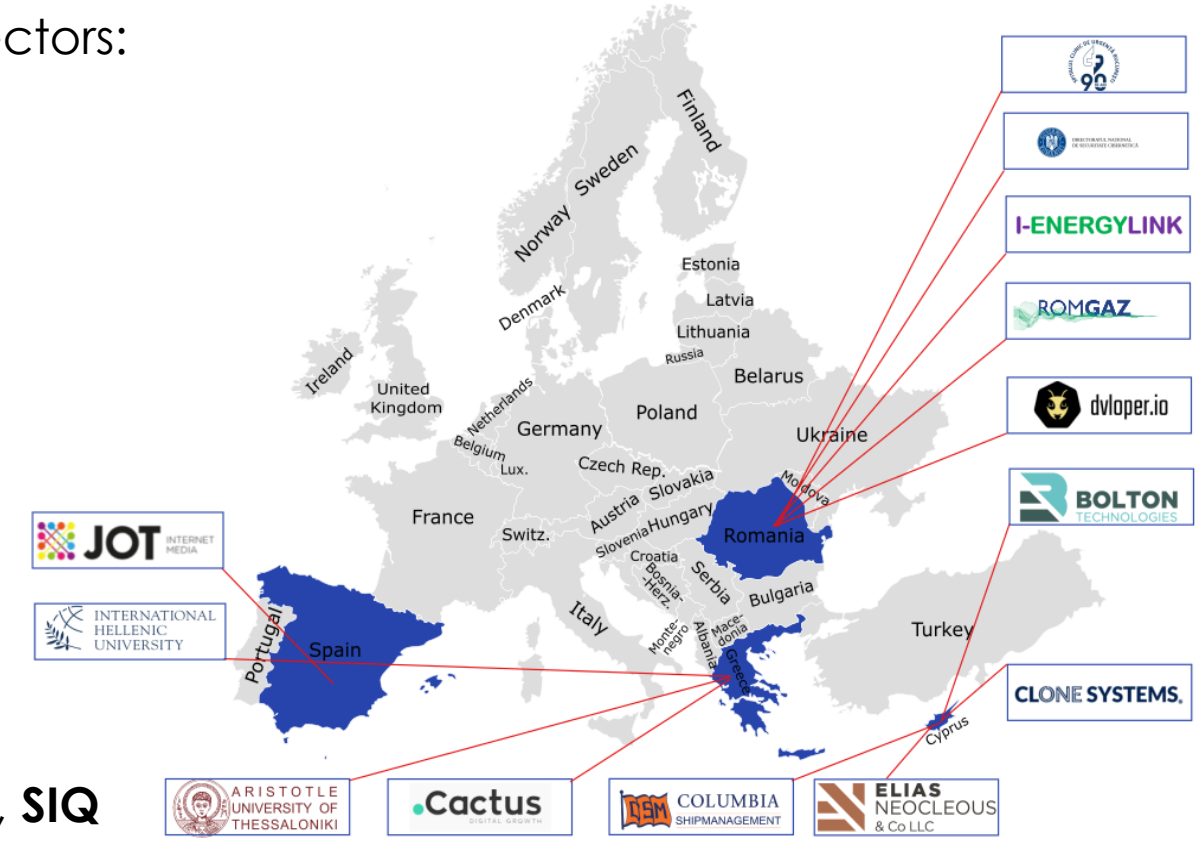
This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

Consortium Partners

CYBERGUARD
AI-POWERED DEFENSE

13 Consortium Partners Organizations, from different sectors:

- ✓ 1 Consulting (**I-ENERGYLINK**)
- ✓ 2 Universities (**AUTH**, **IHU**)
- ✓ 1 Governmental (**DNSC**)
- ✓ 1 Healthcare (**SCUB**)
- ✓ 1 Utility (**ROMGAZ**)
- ✓ 1 Shipping (**COLUMBIA**)
- ✓ 1 Legal Service (**ENC**)
- ✓ 1 Media (**JOT**)
- ✓ 4 IT Services & Technology (**BTS**, **CACTUS**, **CLONE**, **SIQ**



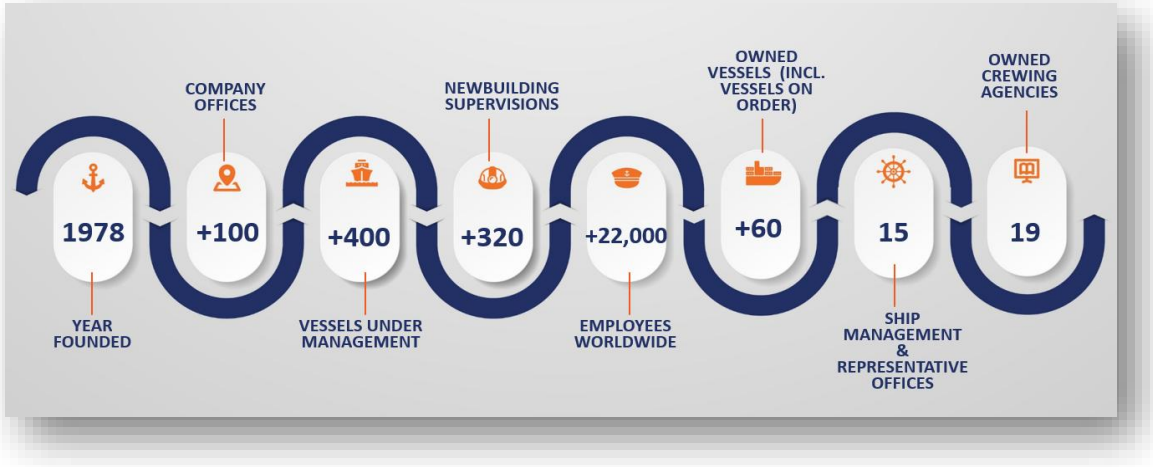
Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Partner Profile Presentation

Columbia Shipmanagement is part of the Columbia Group, a leading global integrated maritime, logistics, leisure and energy platform.



Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

COLUMBIA SHIPMANAGEMENT

Columbia's Role in CyberGuard

CYBERGUARD
AI-POWERED DEFENSE

- **WP2 - Use Case Definition and Scenario Design**
  - Provide real maritime use case scenarios (fleet operations, SOC workflows, vessel–shore communication)
  - Validate functional & non-functional requirements based one the operational and technical challenges found on ships
  - Contribute regulatory alignment (NIS2, IMO, ISO27001)
- **WP5 - Pilot Testing, Platform Validation & Evaluation**
  - Acts as a key maritime pilot partner, hosting real-world use-case demonstrations
  - Supports the setup, execution, and monitoring of pilot scenarios onboard ships or maritime systems
  - Provides operational feedback on usability, functionality, and performance
  - Assists in showcasing the platform's effectiveness to stakeholders and evaluators
- **WP6 – Dissemination, Communication and Exploitation**
  - Dissemination, high impact communication activities and outreach events
  - Stakeholder and community engagement and training towards CyberGuard solution

Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

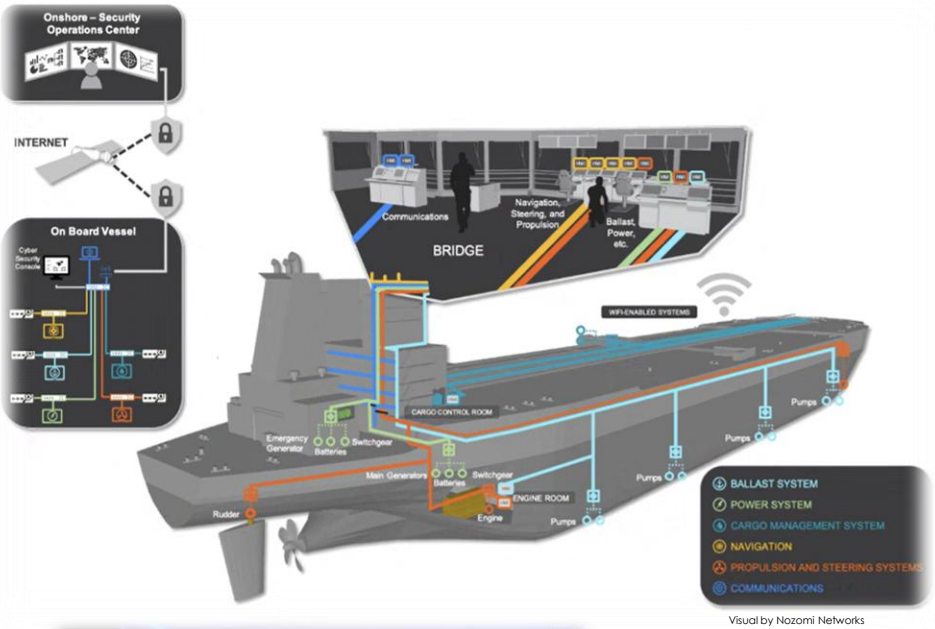
Why Cybersecurity Matters for Maritime

The maritime sector operates within a highly interconnected digital fleet ecosystem, where ships, cloud services, shore-based operations, classification societies, OEM vendors, and global suppliers continuously exchange operational, navigational, and technical data.

Modern fleet operations depend on seamless ship-shore-cloud connectivity, enabling remote monitoring, voyage optimization, predictive maintenance, and crew services - but also expanding the cyber-attack surface.

This creates a complex cyber risk landscape driven by several sector-specific factors:

- Hybrid IT/OT environments onboard ships
- Digitized maritime infrastructure based on the vessel type
- Heavy dependence on third-party vendors and international supply chains
- Growing ransomware and targeted cyberattacks
- Regulatory pressure (IMO MSC.428(98),IACS E26/E27, GDPR, NIS2 etc)



Visual by Nozomi Networks

Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

What CyberGuard intents to cover

CYBERGUARD addresses the operational needs created by different compliance frameworks by providing:

- Intelligent detection & automated threat analysis AI-supported response playbooks
- CTI enrichment mapped to different critical sector risks
- Penetration testing & adversarial simulations
- Incident reporting support – DFIR capabilities
- Compliance assistance

Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

NIS2 – Compliance Requires Skills

NIS2 introduces obligations that directly depend on workforce capability:

- Article 21: Cybersecurity risk-management measures
- Article 23: Incident reporting (24h / 72h / 1 month)
- Article 20: Management accountability & cybersecurity training
- Article 32: Security audits

Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

COLUMBIA SHIPMANAGEMENT

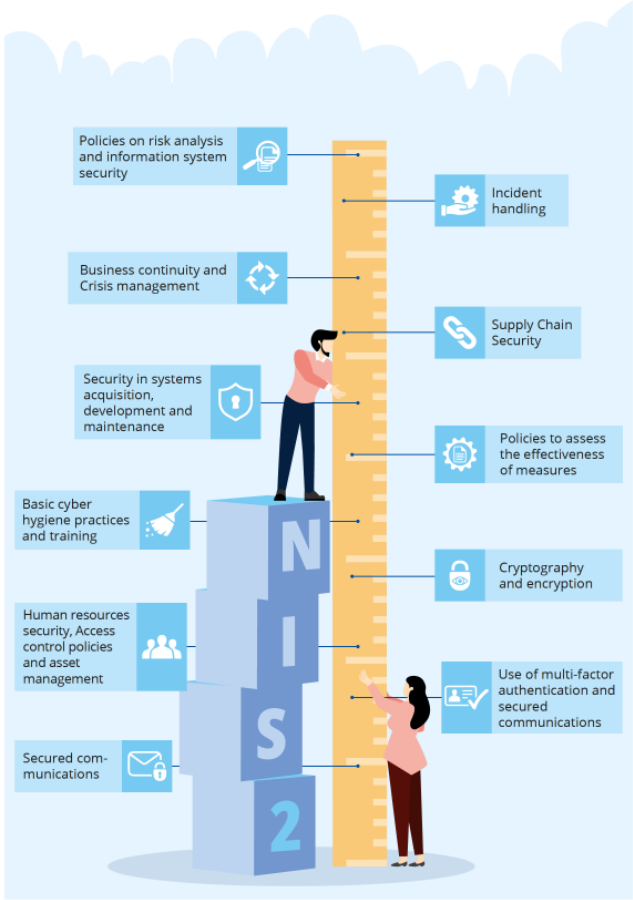
The Gap: What Maritime Needs from NIS2

CYBERGUARD AI-POWERED DEFENSE

To meet the expectations of NIS2, the maritime sector must develop a set of core cybersecurity capabilities, including:

- Competent cybersecurity functions across ship and shore to handle:
  - Security Monitoring – SOC Oversight
  - Incident Response and Containment
  - Digital Forensics and Evidence preservation
  - CTI interpretation for cross sector threat scenarios
  - Compliance Reporting and Documentation
  - Risk Assessment and Continuous Monitoring

- ECSF aligned workforce development to ensure that fleet and shore IT are properly trained and role based responsibilities are assigned
- Efficient IR workflows capable to support NIS2 strict timelines



Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

COLUMBIA SHIPMANAGEMENT

ECSF Roles activated by CyberGuard

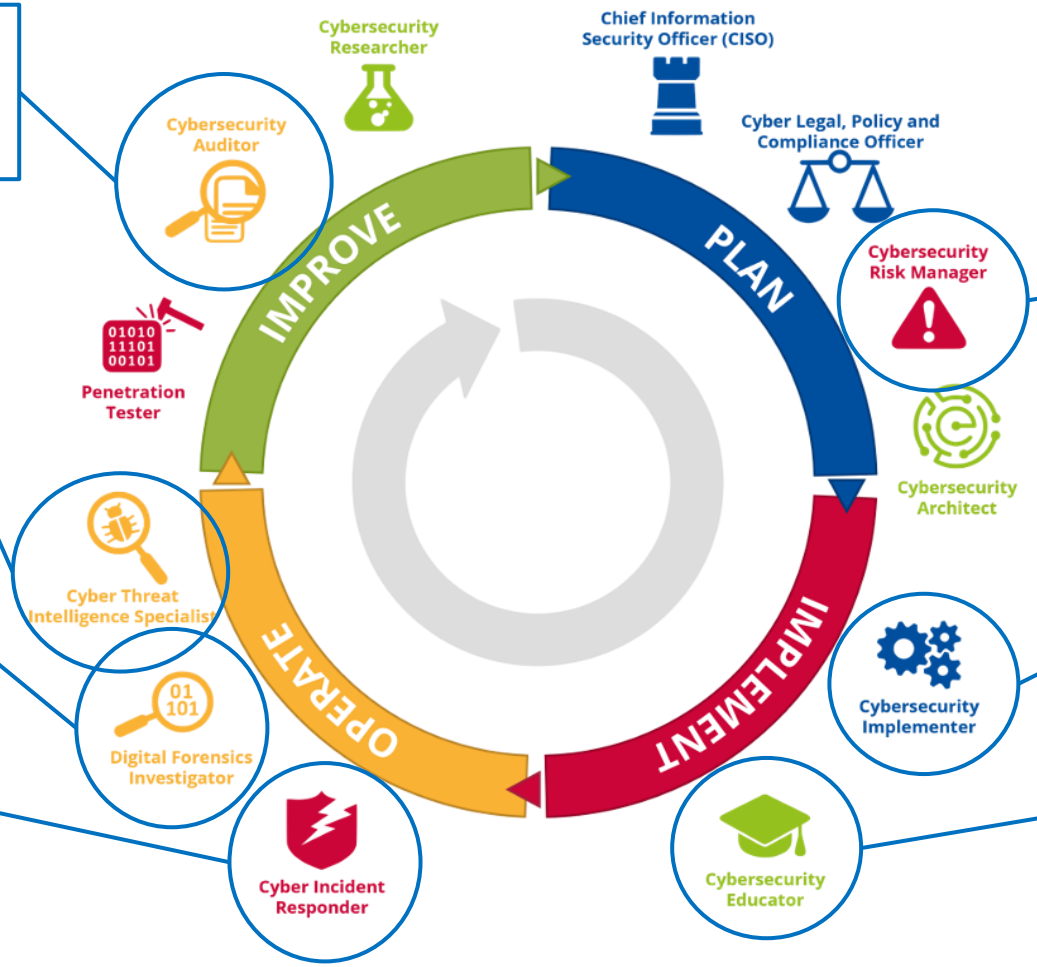
CYBERGUARD AI-POWERED DEFENSE

Use tool capabilities to perform checks policy violations Art.32

Cross CTI for critical sectors Art.23/29 (NIS2)

Evidence Collection Support Art.23 (NIS2)

IR Workflows + AI Playbooks Art.23 (NIS2)



Maritime Risk Scenarios Art.21 (NIS2)

Secure Configuration Testing Art.21 (NIS2)

Training in cyber-range sessions Art.20/21 (NIS2)

Co-funded by the European Union

This project has received funding from the European Union's Digital Europe Programme, under Grant Agreement no. 101190251.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Thank You!

MARIOS IOANNOU
GROUP BUSINESS INFORMATION SECURITY OFFICER

COLUMBIA SHIPMANAGEMENT