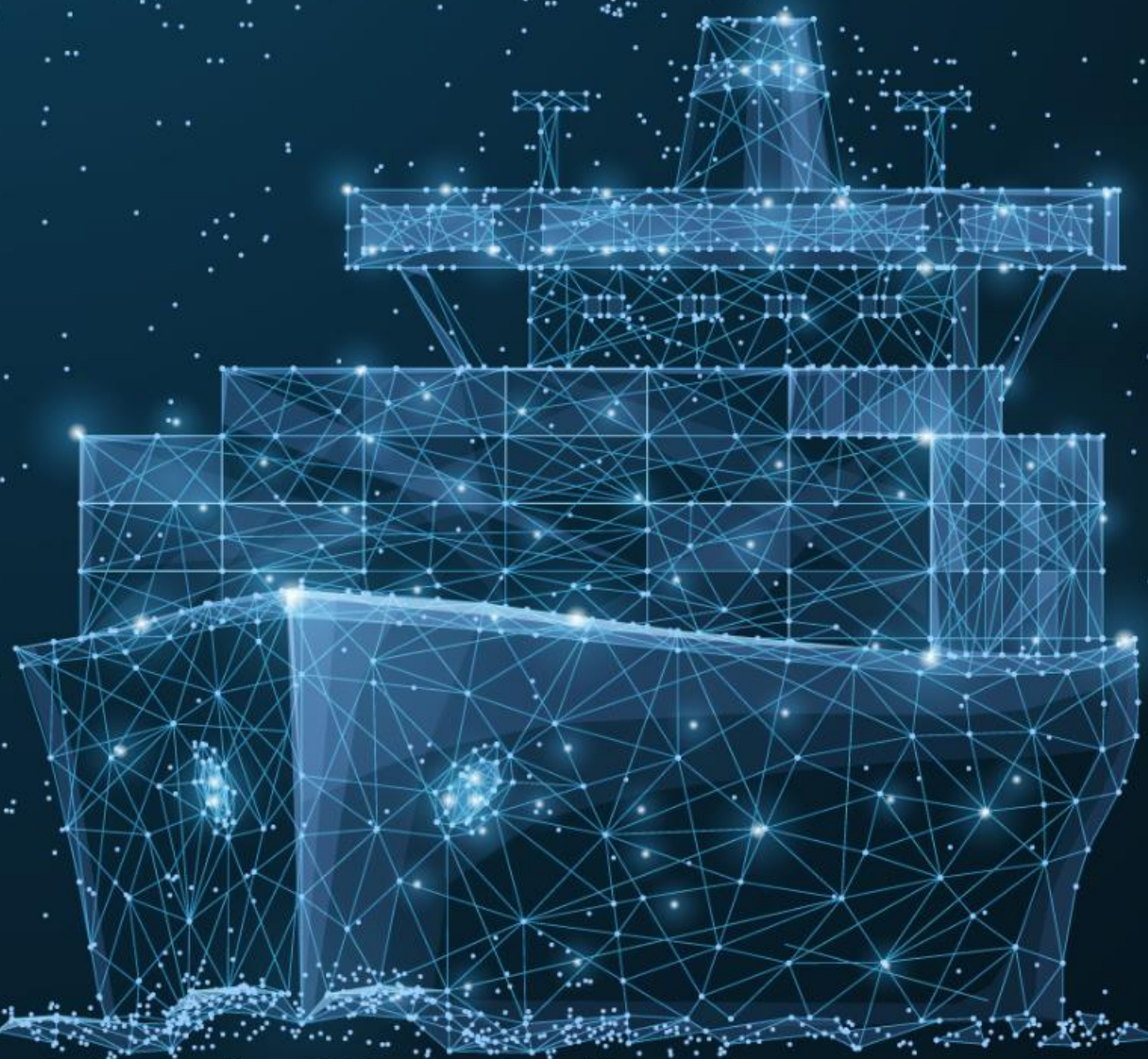
Welcome!

CyberMAR

Pilot Demonstration
&
Final Event

16 December 2022
Hybrid Event



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.

Event rules

- The event will be recorded
- Your microphones and cameras will be kept off
- You can provide your questions in the chat. They will be answered during an interactive discussion session at the end of the event

Many thanks for your participation and cooperation!

Agenda

Session Time Slot (CET)	Session Title
09:00 - 09:30	**Welcome coffee**
09:30 - 09:40	Welcome
09:40 - 10:00	Event and Cyber-MAR Introduction
10:00 - 10:30	Cyber-MAR Overview and Benefits
10:30 - 10:45	**Coffee Break**
10:45 - 12:45	Piraeus Pilot Demonstration
12:45 - 14:15	**Lunch Break**
14:15 - 14:30	MaCRA and Impact on Port Operations
14:30 - 14:45	Econometric Model and Wider Economic Impacts
14:45 - 15:15	Cyber-MAR Training Program
15:15 - 15:30	**Coffee Break**
15:30 - 15:45	Exploitation of project results
15:45 - 16:15	FORESIGHT: Concept, Objectives, Results
16:15 - 16:30	Conclusion and Discussion
End of meeting	

Cyber-MAR Final and Piraeus Pilot Event

Welcome and Event Introduction

Eleftherios Ouzounoglou, ICCS

16th December 2022

Motivation

- The maritime sector is one of the most **important financial sectors** for the European Economy
  - With over 80% of goods transportation in volume carried by sea, ports are **key infrastructures** within the logistics value chain
- Ports and ships are being **digitized** at a very fast pace to address the challenges of the globalized and competitive economy
- The increasing use of **complex system-of-systems** present many attack surfaces and over the last decade there has been a significant increase in the number of disclosed **cyber-attacks**
  - Antwerp Port case, Port of Barcelona (2017), Maersk NotPetya (2018), CMA Ransomware (2020), PLA DDoS (2022)
- The cyber-resilience of ports is essential to **prevent** possible **disruptions** to the economic supply chain

Motivation

- Maritime-specific **cybersecurity risk assessment** has become essential creating a growing need for **raising cybersecurity awareness** in the maritime sector.
- **Cyber Ranges** are recognized as efficient tools
  - to raise cybersecurity **awareness**
  - to increase stakeholders' **operational experience** through training
  - to provide a valuable **prevention** measure through the realistic simulation of the ports' IT and OT infrastructures

The major role of the ports in the supply chain logistics has led our consortium to propose the Cyber-MAR project focusing on port cyber-risk assessment, awareness raising and training to enhance port cybersecurity capabilities

About | Project Facts

Title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain.

Topic: SU-DS-2018: Cybersecurity preparedness-cyber range, simulation and economics

Contracting Authority: European Commission H2020

Project ID: 833389

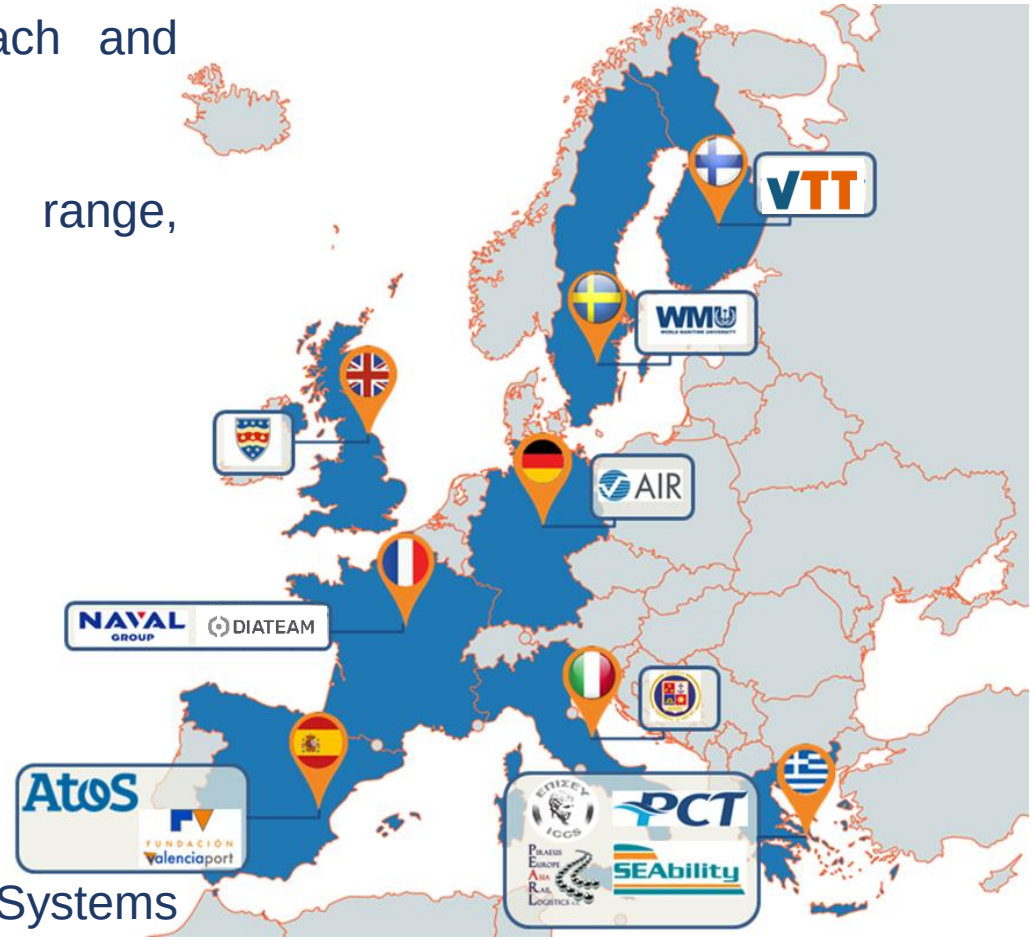
Funded scheme: IA – Innovation Action

Duration: From 2019-09-01 to 2023-02-28

Total cost: EUR 7 154 505.00

EU contribution: EUR 6 018 367.507

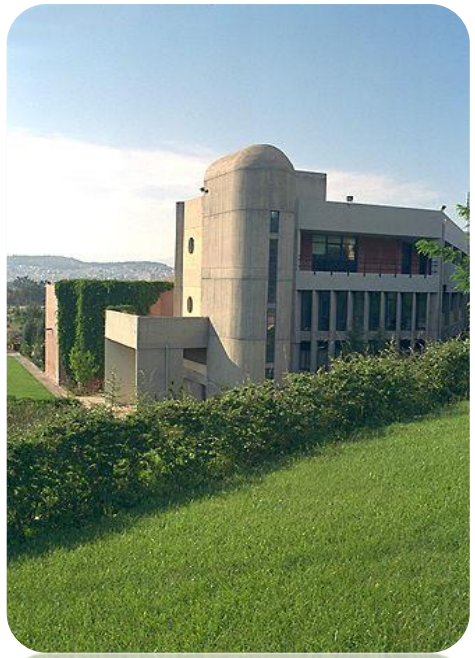
Coordinator: Institute of Communication and Computer Systems (ICCS), Greece

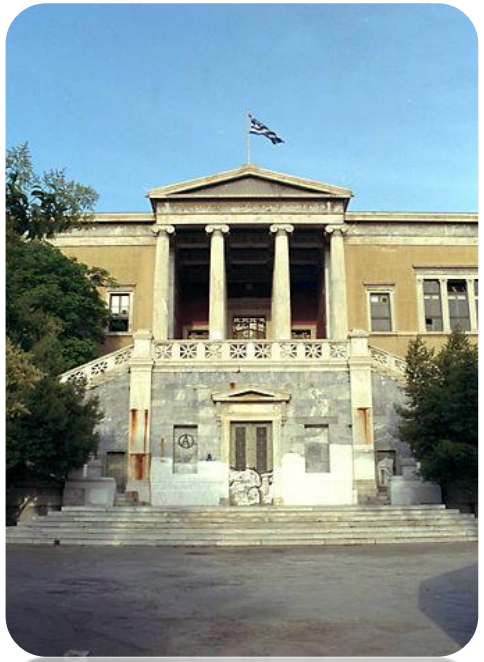


Institute of Communication and Computer Systems

ICCS stands for the Institute of Communication & Computer Systems, Athens, Greece.

A public scientific & technological institute which undertakes advanced research in the field of electrical, electronic and computer engineering & technologies.





- Electrical engineering
- Fusion and Perception Tools
- Signal and image processing
- Intelligent Transportation Systems
- E-mobility
- Electric vehicles
- Human-machine interactions
- Virtual Reality
- Simulation and modeling
- H/W, digital and analog electronics
- S/W engineering and computer technologies
- Control and robotics
- Bioengineering
- Microwave and optical sensors
- Telecom

Major Project Results

- Developed an innovative platform that extends the capabilities of Cyber Ranges for increasing cyber awareness and preparedness level, validating business continuity management and minimizing business disruption potential of maritime logistics value chain actors
- Integrated a Learning Management System for providing a cost effective and easily accessible training environment that covers the needs of the maritime domain
- Deployed and interconnected cyber risk analysis and econometric models to support decision making for cybersecurity measures
- Established collaboration with CERT/CSIRTs networks and tested operational ways to analyse cybersecurity data and information collected
- Validated and evaluated our solution in three pilot use cases (2 ports and 1 ship simulation environment)

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Eleftherios Ouzounoglou, ICCS

eleftherios.ouzounoglou@iccs.gr

This project has received funding from the European Union's horizon 2020 research and innovation programme under grant agreement No. 833389