Cyber-MAR: An Overview

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

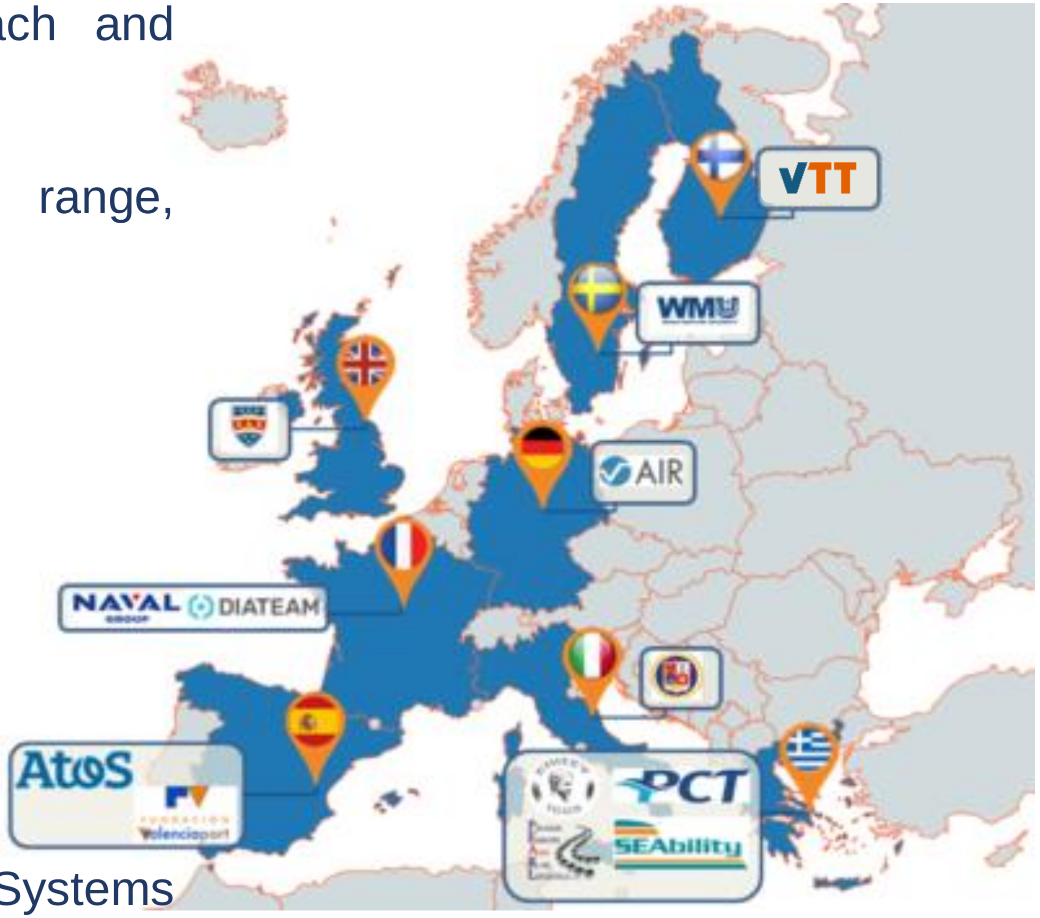
Funded scheme: IA – Innovation Action

Duration: From 2019-09-01 to 2022-08-31

Total cost: EUR 7 154 505.00

EU contribution: EUR 6 018 367.507

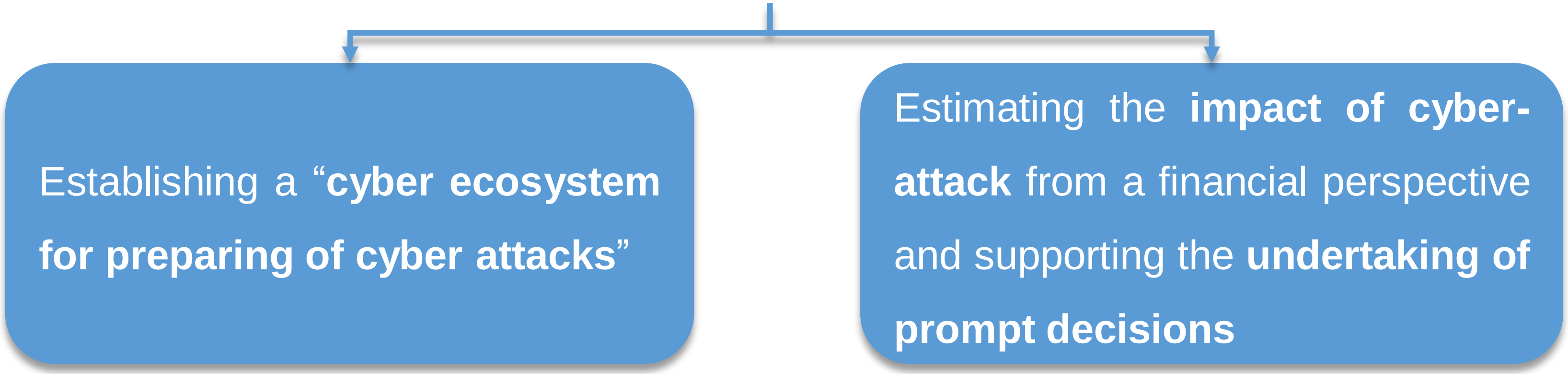
Coordinator: Institute of Communication and Computer Systems (ICCS), Greece



Challenges & Goal

- **Maritime information systems** in many cases designed without accounting for the **cyber risk**
- **Digital infrastructure** has become essential & critical to the **safety** and **security** of shipping and ports
- Importance of **handling cyber preparedness** as a highly prioritized aspect is paramount
- Estimation of accurately cybersecurity investments based on valid risk and econometric models

Cyber-MAR ultimate goal unfolds in **two main directions**:



Establishing a "**cyber ecosystem for preparing of cyber attacks**"

Estimating the **impact of cyber-attack** from a financial perspective and supporting the **undertaking of prompt decisions**

Cyber-MAR Key Objectives (1/2)

O1. Enhance the **capabilities** of cybersecurity professionals and **raise awareness** on cyber-risks

Deploy Cyber-MAR Range, training modules through LMS, improvement in response times in specific resilience metrics

O2. Assess cyber-risks for operational technologies (OT)

Maritime Cyber-Risk Assessment deployment and integration in Cyber-MAR platform

O3. Quantify the **economic impact** of cyber-attacks across different industries with focus on **port disruption**

Quantify economic risk in terms of Time-to-Recover or Product Value at Risk, integration in Cyber-MAR platform

Cyber-MAR Key Objectives (2/2)

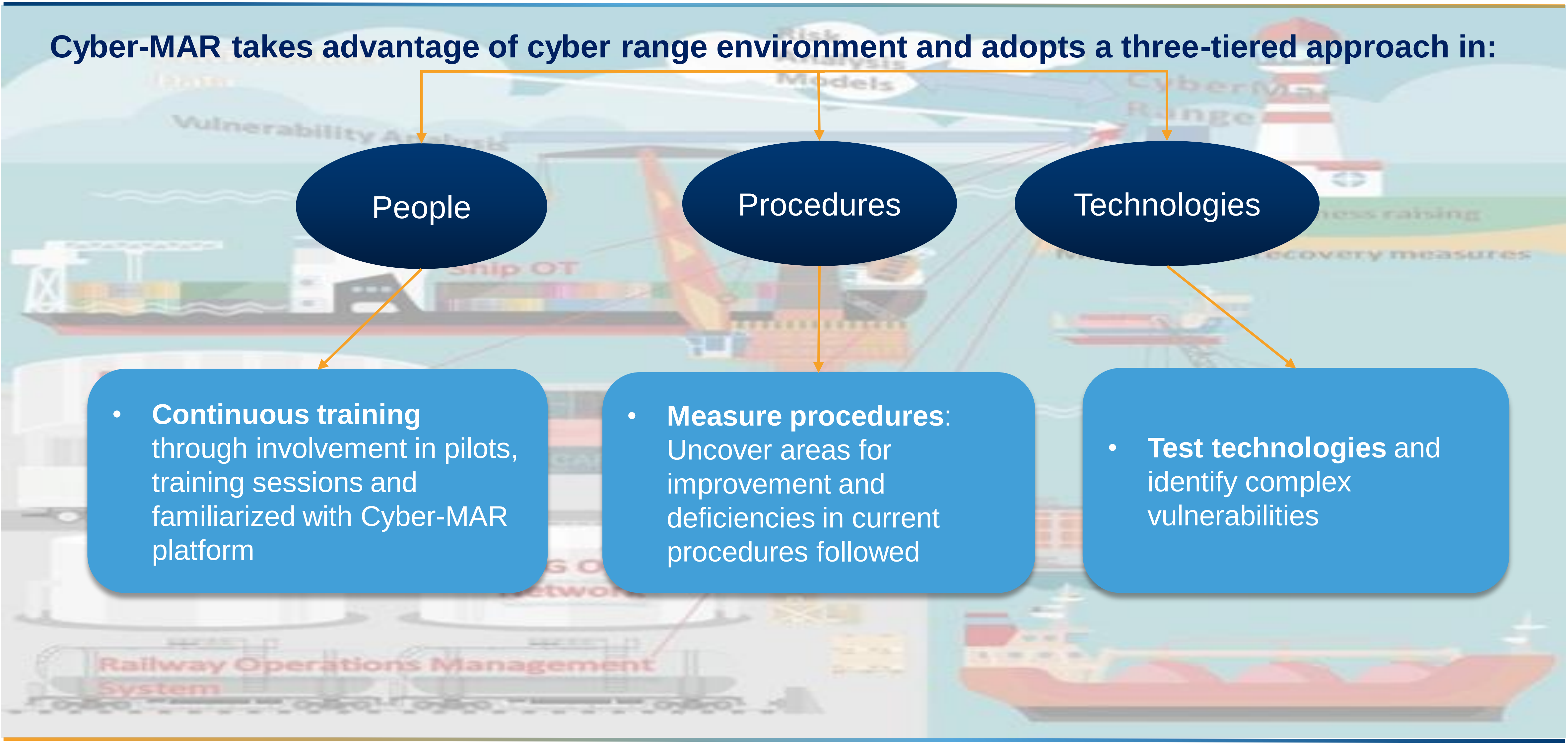
O4. Promote **cyber-insurance market maturity** in the maritime logistics sector (adaptable to other transport sectors as well)

Develop recommendations based on findings and outcomes from Cyber-MAR pilots and simulations

O5. Establish and **extend** CERT/CSIRTs, competent authorities and relevant actors **collaboration** and **engagement**

Create a maritime Malware Information Sharing Platform (MISP) community, engage at least 2 CERT/CSIRTs in pilot activities

Cyber-MAR Concept & Methodology



Cyber-MAR takes advantage of cyber range environment and adopts a three-tiered approach in:

People

Procedures

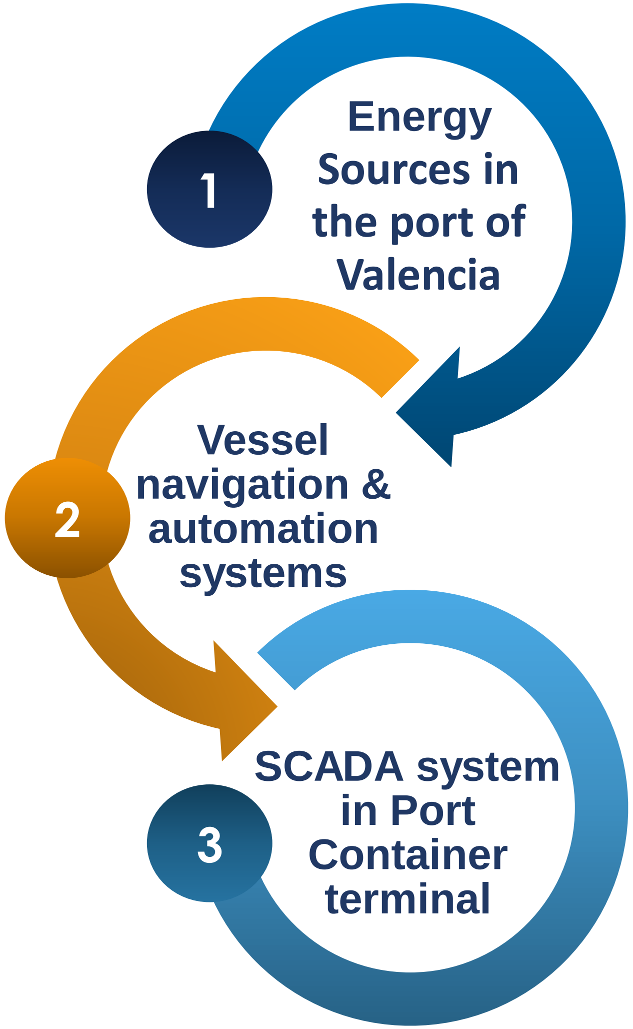
Technologies

- **Continuous training** through involvement in pilots, training sessions and familiarized with Cyber-MAR platform

- **Measure procedures**: Uncover areas for improvement and deficiencies in current procedures followed

- **Test technologies** and identify complex vulnerabilities

Pilot Scenarios


1
Energy Sources in the port of Valencia
2
Vessel navigation & automation systems
3
SCADA system in Port Container terminal

The Cyber-MAR platform will be applied to simulate **the port electrical grid of the port of Valencia**, including protocols for protecting the grid and crisis management after attack.

The Cyber-MAR platform will be applied to simulate **a ship bridge cyber-attack**, including potential attacks to navigation, communication and control systems.

The Cyber-MAR platform will be applied to simulate **a SCADA attack to the Port Container Terminal of Piraeus Port**. In particular, the consequences of a cascade effect extending the attack to the railway operator network.

Expected Impacts

Impact on Resilience to Cyber-Threats & Data Privacy Breaches

Enhancement of the **resilience of target organizations** to new and emerging threats through the **identification of recurring or emerging patterns of cyber-attacks** and **privacy breaches** with a decent degree of accuracy.

Impact on Supply Chain Efficiency

Cyber-MAR aims to offer the potential to **big players of logistics domain** to **join forces on estimating cyber-risk** and **mitigate** such **threats**, while **fostering open tools** that will improve the internal processes within each organization.

Impact on Appropriate Investments for Cyber-Security

Cyber-MAR focuses on the provision of a fully customizable and tailored view on the trade-offs, aims to **increase the available open tools** in number and variety, while offering an **intuitive integration to all** (physical and virtual) **IT components**.

Societal Impact

Cyber-MAR overemphasizes the importance of **accessible training infrastructures for cyber-defense**, in OT, transport and logistics domains and at the same time aims to contribute to the **standardization efforts** to make such issues prominent in the society.

Cyber-MAR Target Audience

- Decision Makers, Public Authorities and International Organizations
- Academia
- Port authorities, operators and associations
- Freight transport and Logistics actors
- CERT/CSIRTs network
- Insurance, Shipping and Cybersecurity companies/enterprises
- European and International organizations & networks for cybersecurity

Contact us

If you have any questions or require further information please contact us:

Address: Angelos Amditis
Institute of Communication and Computer Systems –
ICCS, NTUA, Building of Electrical Engineers, Office 2131
9, Iroon Politechniou Str.
GR-15773, Zografou Athens, GREECE

Tel: +30 2107722398

email: a.amditis@iccs.gr, info@lists.cyber-mar.eu

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Speaker, Institution

✉ Contact details of the speaker

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