At a glance

Cyber-MAR is an effort to **fully unlock** the value of the use of cyber range in the maritime logistics value chain via the development of an innovative **simulation environment** adapting in the peculiarities of the maritime sector but being at the same time easily applicable in other transport subsectors. A combination of innovative technologies are the technology enablers of the proposed Cyber-MAR platform which is not only a **knowledge-based platform** but more importantly a **decision support tool** to cybersecurity measures, by deploying novel risk analysis and econometric models. CSIRTs/CERTs data collected will be analysed and feed the knowledge-based platform with new-targeted scenarios and exercises. Through Cyber-MAR, the maritime logistics value chain actors will **increase**their **cyber-awareness level;** theywill validate their business continuity management **minimizing business disruption potential.** Cyber-MAR will act as a **cost-efficient training solution** covering the maritime logistics value chain.

Cyber_MAR

Cyber-MAR

Cyber-MAR EU Project

info@lists.Cyber-MAR.eu

www.cyber-mar.eu

Consortium

ΕΠΙΣΕΥ ICCS

Atos

SEAbility

ITALIAN SHIPPING ACADEMY

AIR

UNIVERSITY OF PLYMOUTH

DIATEAM

PCT

FUNDACIÓN VALENCIAPORT

NAVAL GROUP

VTT

PIRAEUS EUROPE ASIA RAIL LOGISTICS S.A.

WMU WORLD MARITIME UNIVERSITY

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Cyber MAR

cyber-mar.eu

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

The Objectives

IN ORDER to be well prepared for emerging and future cyber-attacks, efficiently mitigate risks and follow an as much as accurate and cost-efficient cyber-defense investment plan, maritime logistics actors need to base their cyber defense strategy on palette of innovations, novel combinations of them and changes of mindset, reflected in the following Cyber-MAR high-level objectives:

- Enhance the capabilities of cybersecurity professionals and raise awareness on cyber-risks
- Assess cyber-risks for operational technologies (OT)
- Quantify the economic impact of cyber-attacks across different industries focusing on the maritime logistics value chain
- Promote cyber-insurance market maturity in the maritime logistics sector (adaptable to other transport sectors as well)
- Establish and extend CERT/CSIRTs, competent authorities and relevant actors collaboration and engagement

Facts

Call Identifier: SU-DS01-2018
Duration: From 2019-09-01 to 2022-08-31, on-going project
Total Cost: EUR 7.154.505
EU contribution: EUR 6.018.367

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

Impacts

Enhanced Resilience to Cyber-Threats & Data Privacy Breaches

The prediction of cyber-attacks and their impact and mitigation constitutes a great challenge for the organizations.
Cyber-MAR aims to enhance 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. Also Cyber-MAR platform offers complete **integration among virtual and real OT components** of each organization.

Increased appropriate Investments for Cyber-Security

For SME's cybersecurity products are considered as a luxury, while OT experts face the cumbersome task of cybersecurity tools integration.

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) **OT components.**

Augmented Supply Chain Efficiency

The supply chain as an ideal environment for cyber-attacks and cascading effects are inevitable, causing detrimental effects to cargo delivery times and resources.

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.

Societal Impact

Despite cyber-security measures, large utility infrastructures and transport hubs are primary targets and still prone to unforeseen attacks.

Cyber-MAR overemphasizes the importance of **accessible training infrastructures for cyber-security,** both in IT transport and logistics domains, while aiming to contribute to the **standardization efforts** to make such issues prominent in the society.

Scenarios

1 Energy sources in the port of Valencia

The attack scenario is focused on a local or remote access attack on **energy management system,** simulating the normal operation of the electrical grid, while onsite manual intervention is altering the process. The main objective of this attack is to **cut off the power supply** to the port and avoid the emergency power supply systems from automatically starting up.

2 SCADA system in Port Container terminal

This scenario focuses on the **movement of containers within the terminal.** In particular, the simulation will cover a local access attack on gantry control systems through **wireless maintenance network** and potential disruptions ranging from operational efficiency degradation to life-threatening safety issues due to loss of control of gantry cranes. A risk analysis will be conducted for assessing a cascading effect in the railway provider's network.

3 Vessel navigation and automation systems

This scenario will **simulate** and **validate cyber-attacks** affecting to different vessel systems.