

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 **cyberawareness level**; they will 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



Atos



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 preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain








cyber-mar.eu

Building cyber-resilience within maritime

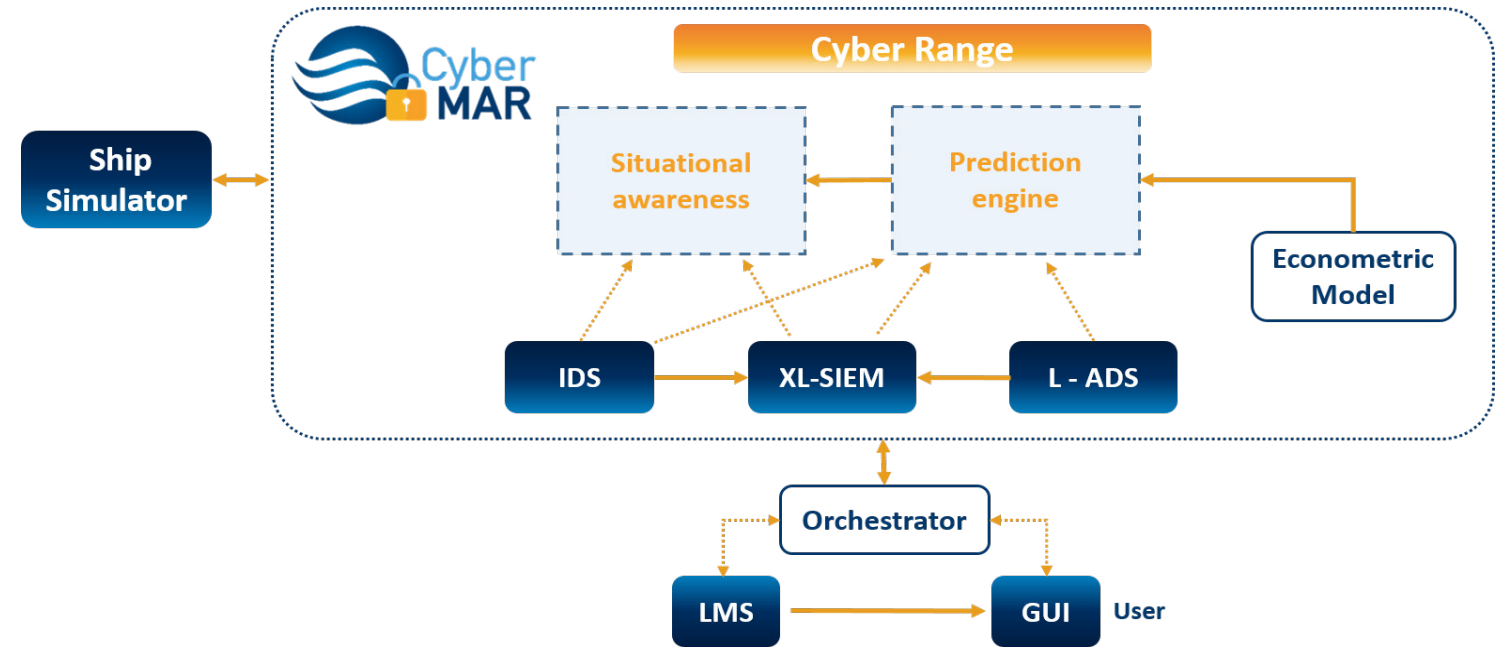


The Objectives

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

Network Simulation



Core components

Cyber-MAR Cyber Range (CR)

This comprises all the technologies, tools and methodologies (hybrid coupling, IDS/IPS, data analytics and intelligence extraction, interconnection system to real automation equipment, networking with additional CRs and simulating environments module, situational awareness) related to the simulation environment, which will be deployed.

Cyber-MAR Learning Management System (LMS)

This comprises technologies and tools related to the MOOCs, which will be developed within the project (training management component, content description processing, training database containing all. The resources and data needed for content generation and

environment creation).

Cyber-MAR Econometric Model (EM)

This comprises the econometric model that will assess the potential economic impact across different value chains due to various cyber-attack scenarios. The economic loss outputs from this module would be used in developing risk mitigation strategies.

Cyber-MAR risk analysis models (MaCRA)

MaCRA (Maritime Cyber-Risk Assess-



ment) framework will assess ship cyber risk by evaluating threats. This module will be integrated within Cyber-MAR platform serving as the risk model component of the system.

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:

Dr Angelos Amditis, Institute of Communication and Computer Systems (ICCS) a.amditis@iccs.gr