World Maritime University

European Coast Guard Functions Forum
Cybersecurity Working Group – 05 May 2022

Dr. Monica Canepa, Research Associate

WMU WORLD MARITIME UNIVERSITY

Maritime Cyber-security

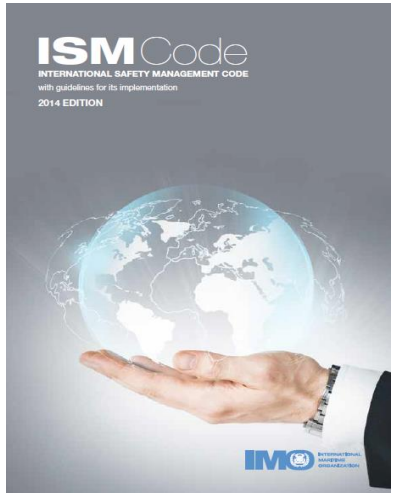
WP LEADER - Training & Awareness Raising with LMS platform integrated to Cyber-MAR CR

Cyber MAR

MARITIME CYBER SECURITY MOTIVATION AND DRIVERS

IMO Legal Framework/ Mandatory Instruments

2002



1993

MSC- FAL 1/ Circ 3
Guidelines on Maritime Cyber risk management

MSC 428 (98) Resolution
Maritime Cyber risk management in safety management system

The Maritime Safety Committee, in June 2017:

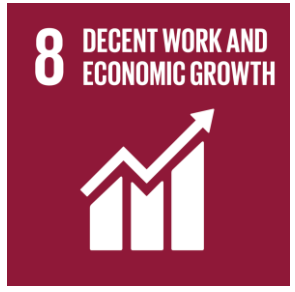
Affirmed that an approved **safety management system should take into account cyber risk management** in accordance with the objectives and functional requirements of the ISM Code;

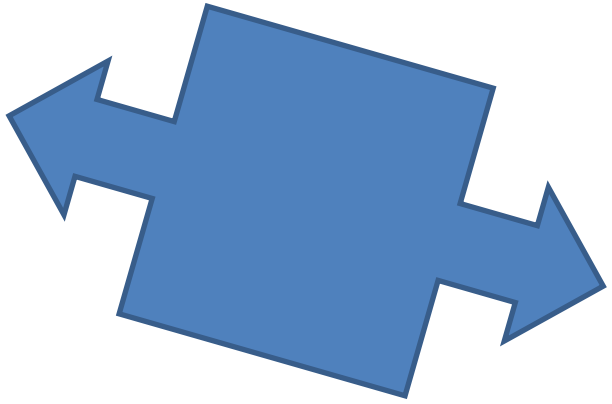
Encouraged Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after **1 January 2021**;

WORLD MARITIME UNIVERSITY

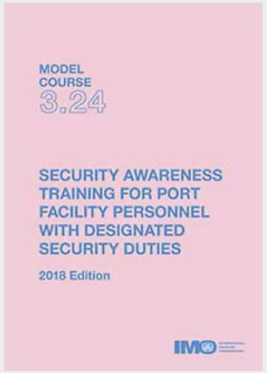
MARITIME CYBER SECURITY MOTIVATION AND DRIVERS

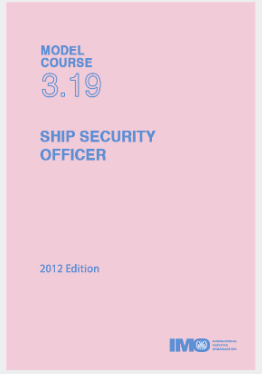
UN2030 Agenda (SDGs 4, 8,9,16 in particular)

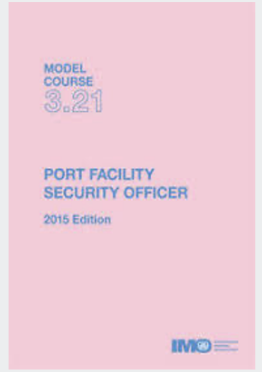




Training of seafarers and shore-based Personnel







IMO is updating its security model courses to incorporate maritime cyber risk management.

Cyber-MAR: An Overview

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)

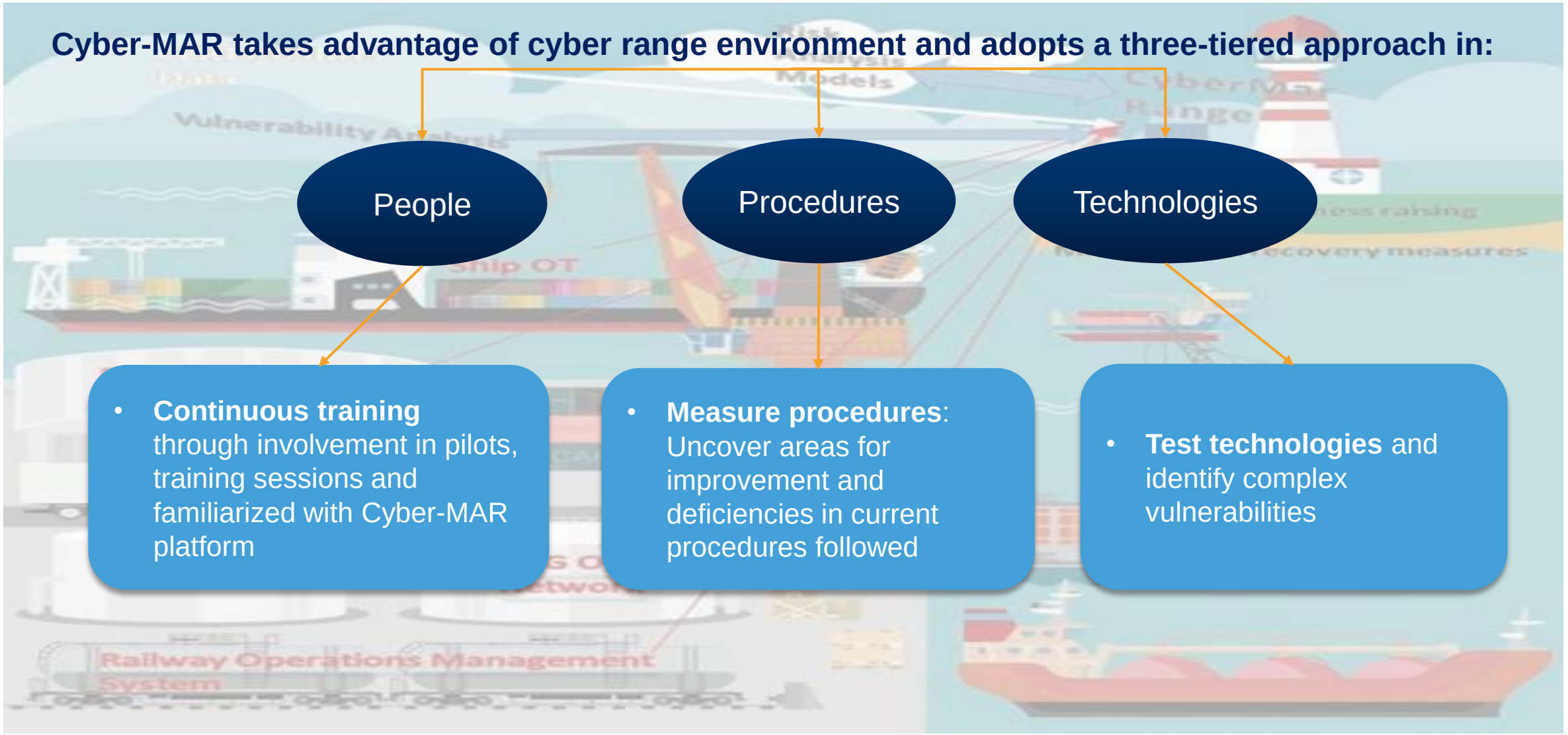
Develop recommendations based on findings and outcomes from Cyber-MAR pilots and simulations

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

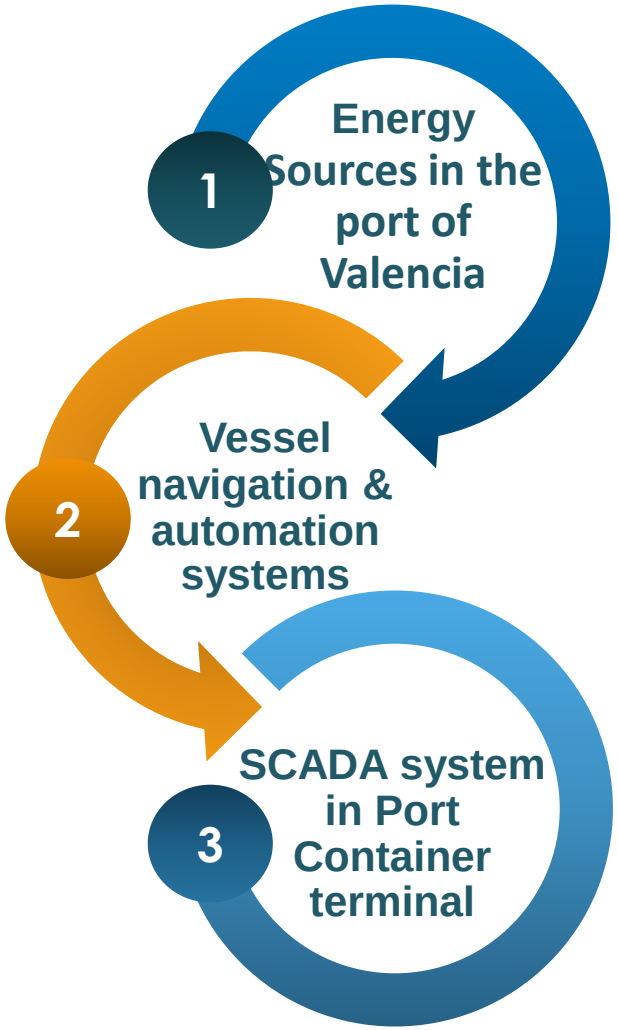
Create a maritime Malware Information Sharing Platform (MISP) community, engage at least 2 CERT/CSIRTs in pilot activities

Cyber-MAR Concept & Methodology

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



Pilot Scenarios



The Cyber-MAR platform will be applied to simulate **the 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.

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

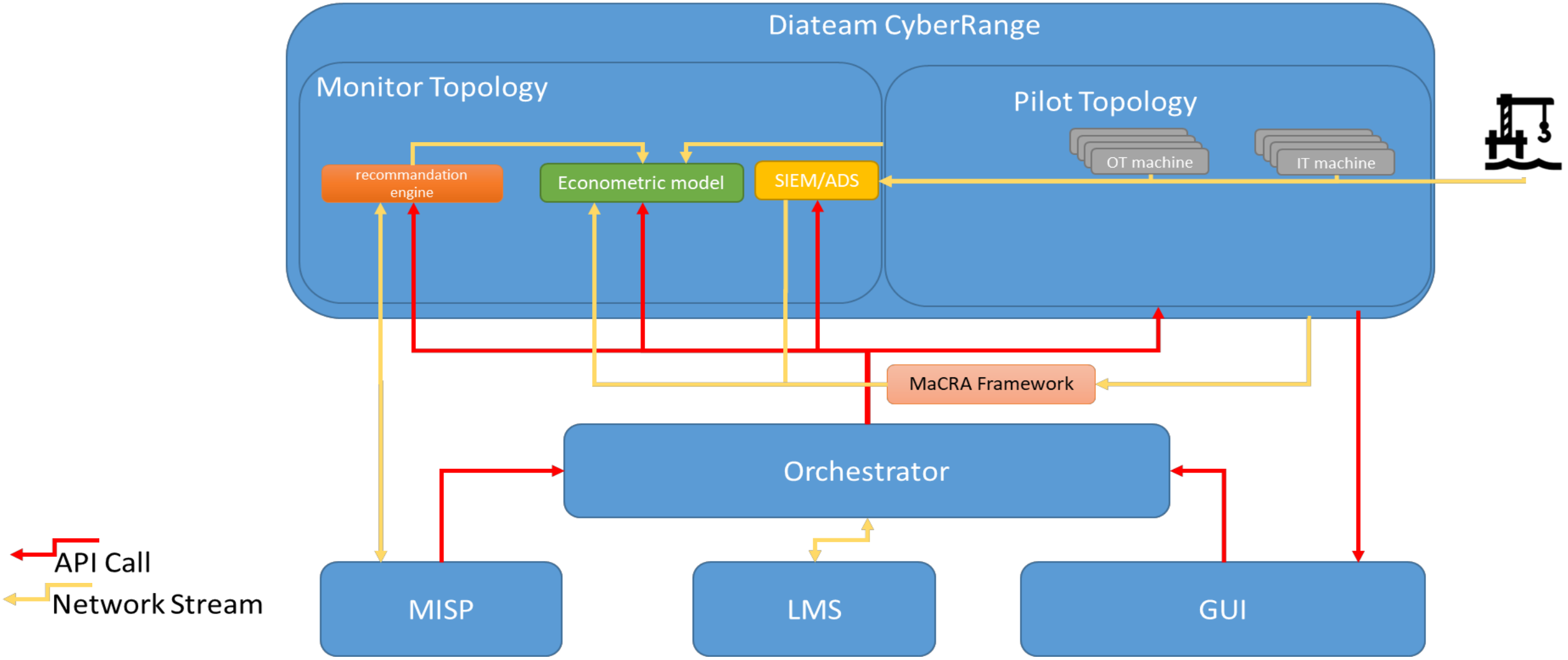
Benefits of using Cyber-MAR

- Adopting a platform like Cyber-MAR can have multiple benefits for an organization, at multiple levels of operation and for different categories of members.

- **Employees**:
  - Experiencing real-world threats in a safe environment
  - Learn how to recognize threats
  - Develop and expand cybersecurity skills
- **Security Operator**:
  - Transfer information from the cyber range for immediate use
  - Measure knowledge and capabilities of internal or external cyber security teams
  - Raise awareness (technical/high level)
  - Penetration Testing exercises
  - Simulate real threat actor TTPs and learn from them
- **Management**:
  - Keep your employees trained
  - Improve overall cybersecurity education
  - Security Assessments in general
  - Test processes and technologies
  - Evaluate Cyber-Risk based also on its economic impact and take cost-effective decisions
- **Research and Development**:
  - Design and Build Prototypes, Testbeds technologies and experimental environments (e.g. IoT, ICS, robotics, smart grids, BigData, VR/AR etc.) and test them against cyber-attacks
  - Design, Develop and Test new tools and methods for Cyber-Security

Cyber-MAR Platform

Architecture



Cyber-MAR Training

Training

https://www.cyber-mar.eu/trainings/

- https://www.cyber-mar.eu/trainings

Trainings

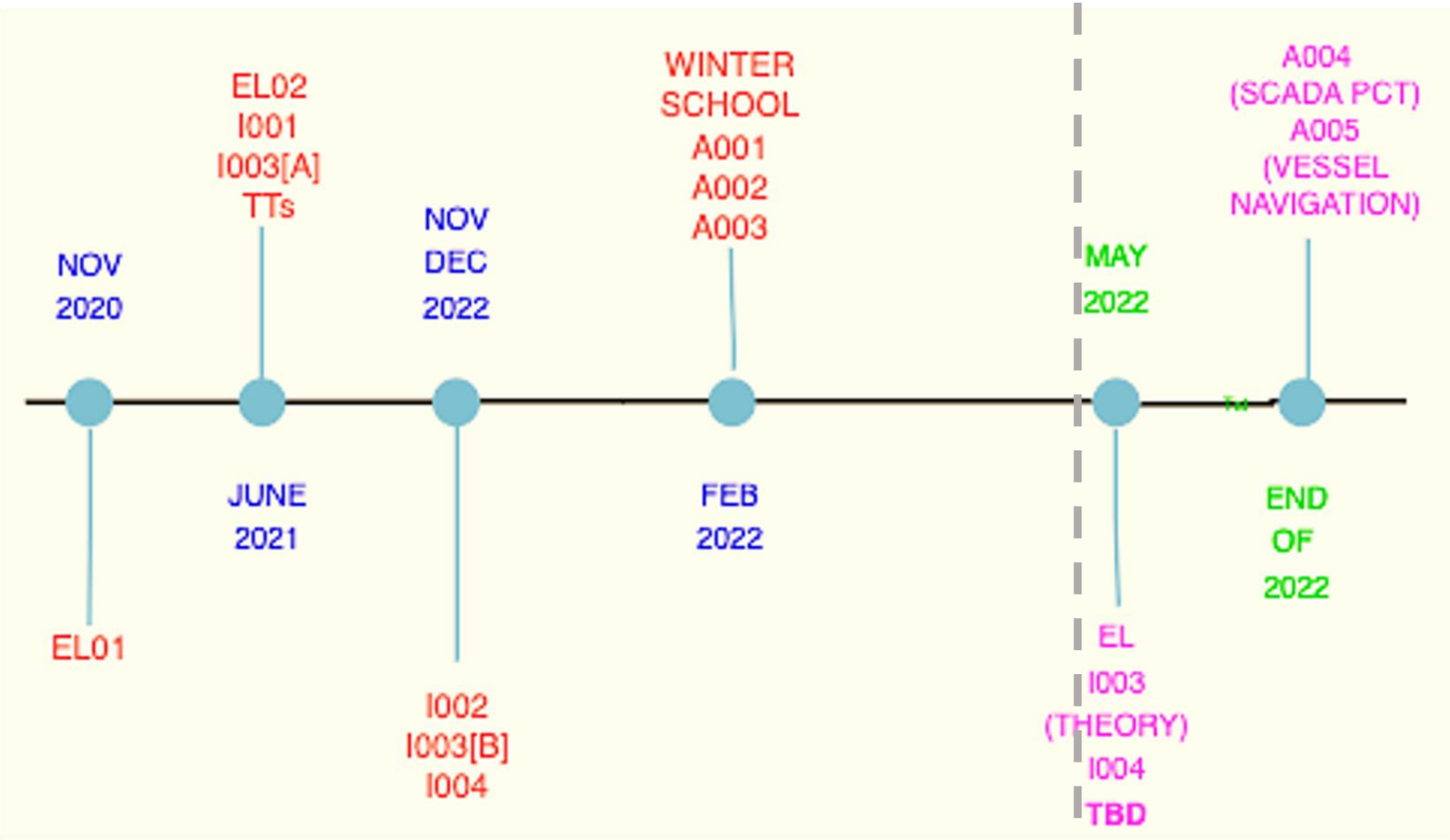
- Entry Level Training
- Mid Level Training
- Advanced Level Training
- Announcements

	Agenda	Download here EL01 Download here for EL02
	Trainers' Bio	Download here EL01 Download here for EL02
	Readings – Cybersecurity with focus on maritime	Restricted Content To view this protected content, enter the password below: Password: ENTER
	Webinar Presentations	Restricted Content To view this protected content, enter the password below: Password: ENTER
		Restricted Content To view this protected content, enter the password

Trainings

- Entry Level Training
- Mid Level Training
- Advanced Level Training
- Announcements

IMPLEMENTED ACTIONS: TRAINING CALENDAR



EL01 - Cybersecurity Awareness
EL02 - Managing Cybersecurity

I001 - Introduction to the Cyber Range
I002 - Basic Tools for a Cyber Range
I003 - Using a Cyber Range to Understand risk
I004 - Lesson learned from Cyber MAR pilots: Cyber- attack scenario on the Valencia port authority's electrical grid

A001 -HNS Pro user training
A002 - Crafting an Attack (Theory)
A003 - Crafting an Attack (Practical)
A004 - Lesson learned from Cyber-MAR pilots: SCADA system in Port Container terminal
A005 - Lesson learned from Cyber-MAR pilots: Vessel navigation and automation systems

TRAIN THE TRAINERS
CTF

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

Thank you for your attention

Monica Canepa, WMU

moc@wmu.se

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