Cyber MAR

Seminar On Trends and Challenges after the Paris Agreement: Global Maritime Technology Cooperation Centre (MTCC)

EU H2020 Cyber MAR project: Cyber security in Maritime Onshore facility

Monica Canepa, World Maritime University

08/10/2019, Malmö

Cyber-MAR Facts & Figures

Name: **Cyber** preparedness actions for a holistic approach and awareness raising in the **MAR**itime logistics supply

Project ID: 833389

Funded under: H2020

Funding scheme: IA - Innovation action

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

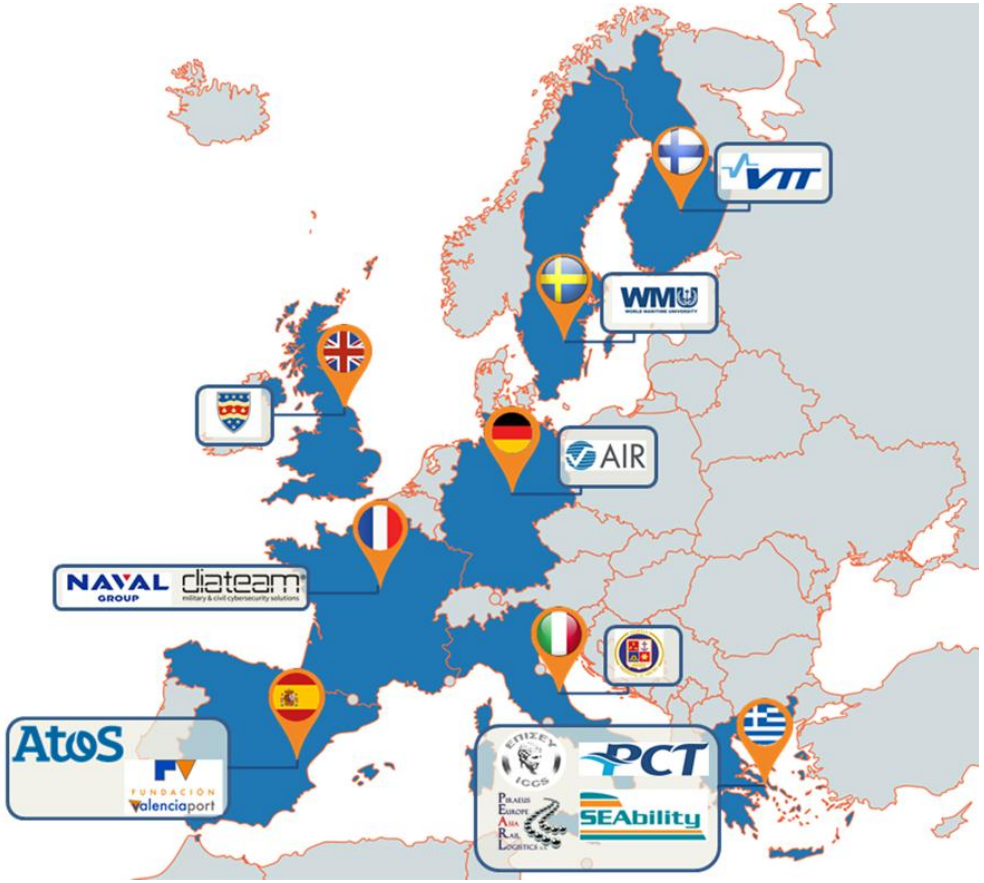
Total cost: EUR 7 154 505.00

EU contribution: EUR 6 018 367.507

Call for proposal: H2020-SU-DS-2018

Topic: SU-DS01-2018 – Cybersecurity preparedness-cyber range, simulation and economics

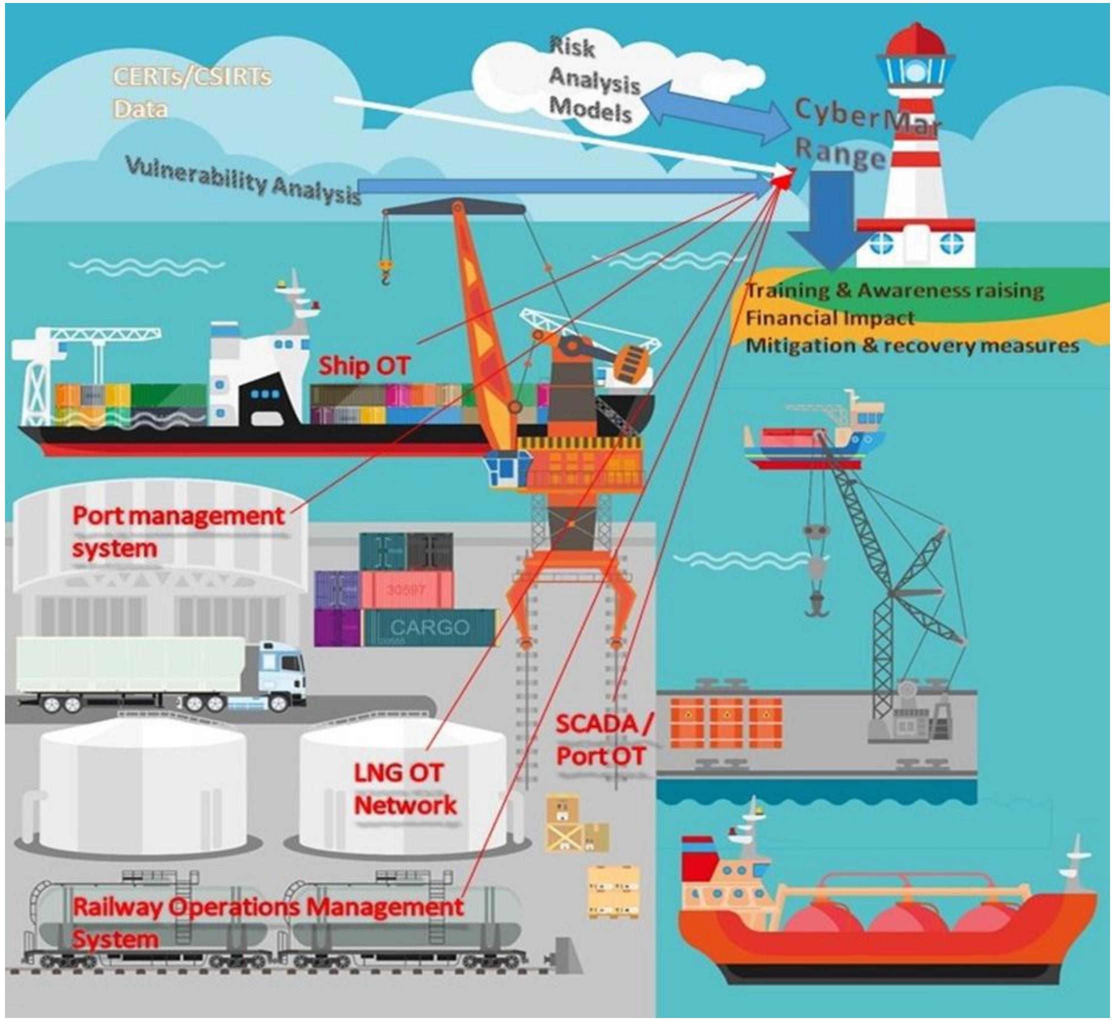
Coordinated by: Institute of Communication and Computer Systems (ICCS), Greece



Cyber-MAR at a glance

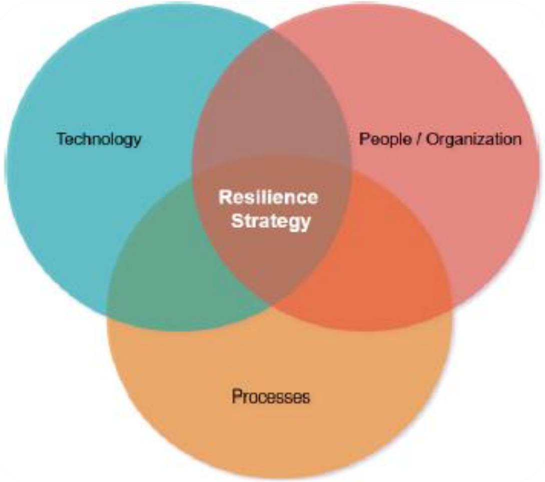
Cyber-MAR takes advantage of cyber range environment and adopts a three-tiered approach targeting at:

- **People:** Continuous training through involvement in pilots, training sessions and familiarised with Cyber-MAR platform
- **Technologies:** Test technologies and identify complex vulnerabilities
- **Procedures:** Uncover areas for improvement and deficiencies in current procedures followed

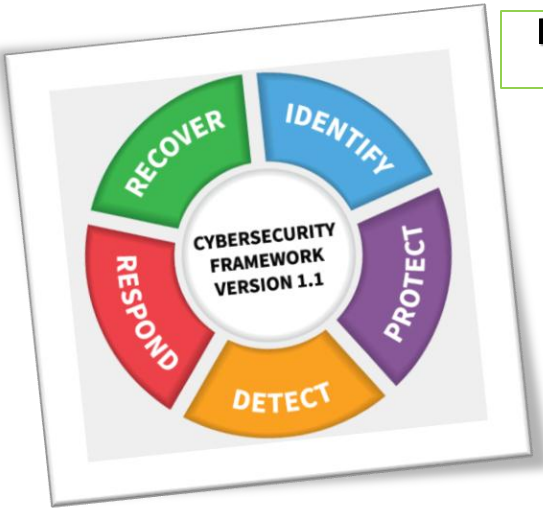


Concept

- Cybersecurity is not only a **technological**, but also a **strategic** and **political** issue
- The NIS directive takes into consideration that...
  - “network and information systems play an essential role in facilitating the goods and people flow.”
  - “existing capabilities are not enough to ensure a high level of security and information systems within the Union”
- High importance of cyber preparedness as a highly prioritized aspect
- By following specific preparedness measures, an organization ensures its service resilience
- The NIST Cyber Security Framework provides a comprehensive approach of cybersecurity, which consists of five steps **: identify, protect, detect, respond and recover**
- Cyber-MAR approach to cyber risk will be aligned with this standard



Main factors of Resilience Strategy



Needs

To be well prepared for **emerging and future cyber-attacks**, efficiently mitigate risks and develop an accurate and **cost-efficient cyber-defence investment plan**, the maritime logistics actors

need to base their **cyber defense** strategy on a set of innovations

Cyber-MAR Objectives

- ❑ **Enhance 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 with a focus on port disruption**
- ❑ **Promote cyber-insurance market maturity in the maritime logistics sector (adaptable to other transport sectors as well)**
- ❑ **Establish and extend CERTs/CSIRTs, competent authorities and relevant actors collaboration and engagement**

Pilot scenarios

Pilot 1: Piraeus Pilot - Cyber Attack via the maintenance wireless network of Piraeus Container Terminal

Pilot 2: Valencia Pilot: The port electrical grid “business process”

Pilot 3: Cyber Attack targeting at navigating instruments (e.g. ECDIS / GPS) - Shipping Operator Pilot

Pilot Valencia Port The port electrical grid “business process”

Cyber-MAR will simulate the port electrical grid, including the whole energy management architecture:

- ✓ software control, SCADAS, PLC´s, instrumentation, actuators, communication systems, etc.

Cyber-MAR will assess a potential cyberattack to the cyber physical systems (CPS), namely IoT, bigdata, blockchain, etc.

Smart grids - overview

Maritime ports are **intensive energy** areas with a plenty of electrical systems that require an average power of many tens of megawatts (MW).

NEEDS: More electricity production **sources**, in particular renewable energies, and also in the improvement of **transport and distribution networks** in order to improve energy reliability and ensure optimum service quality whilst minimizing the frequency and duration of **power cuts.**

Competiveness, profits, reduction of pollution, reliability of operations, carbon emission trading are important energy related considerations for any port authority.

Smart grids in port

What is a smart grid?

Smart grid is a holistic solution that employs a broad range of **information technology** resources

A Smart Grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure **economically efficient, sustainable power system with low losses and high levels of quality, security and safety of supply.**

Why?

Environmental benefits from smart grid implementation in a port area:

❏ Air quality

❏ Less noise

❏ Energy efficient consumption

Smart grids in port

Current technology allows the deployment of a local smart/micro-grid of the size of tenths of MW, capable of islanded operation in case of emergency capable to grant an increasing energy independency.

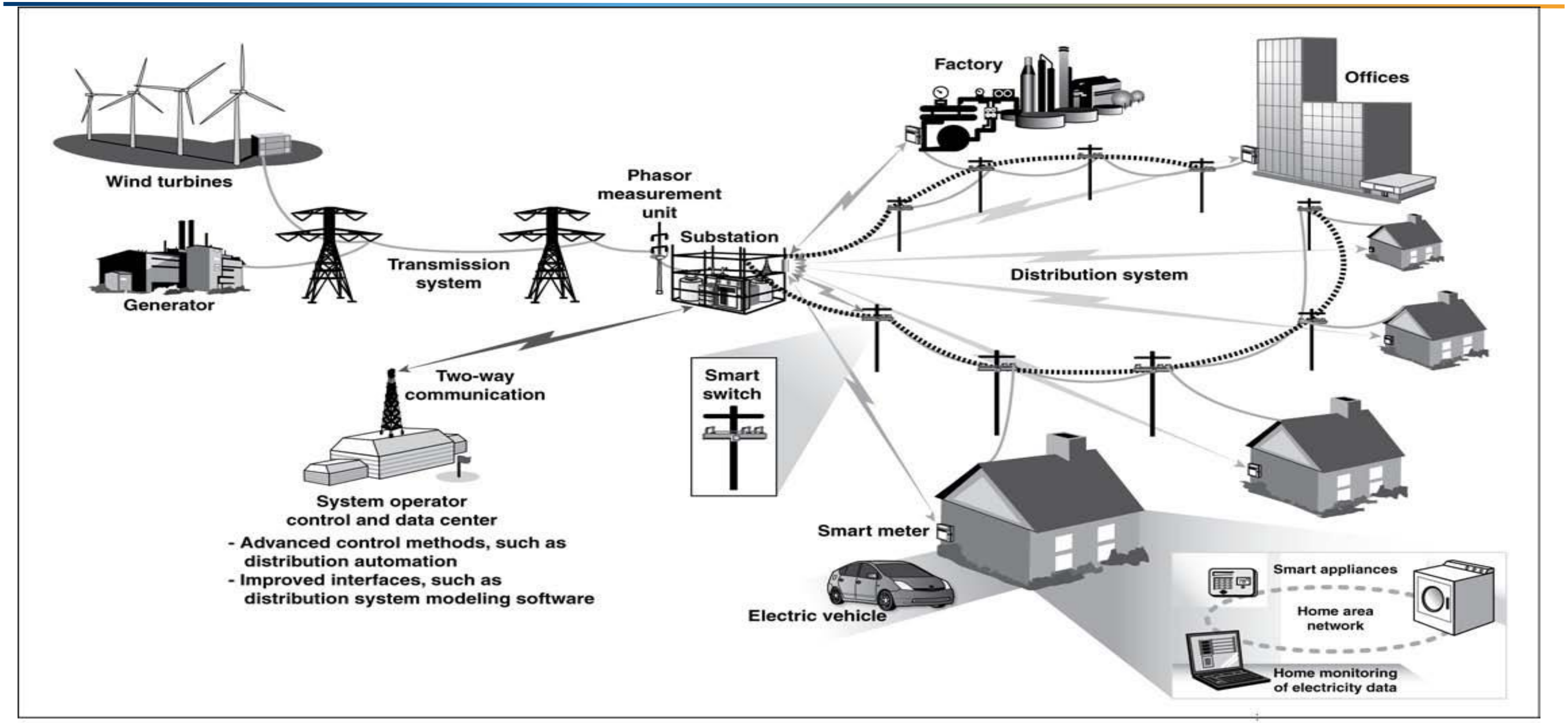
Ownership of the grid permits a large flexibility on prices of energy sold inside the port, trading on local electric market and reduction of pollution.
Renewable energy generation has a large impact on costs since features a low marginal cost.

This pioneer energy model is based on an **optimal energy management** and a **cyber-physical connected port** scenario.

This model supported by IT technologies (big data, IoT, machine learning, etc.) contributes to increase the efficiency in the rationalization of energy consumption

Many ports are using an internal electrical grid connected to an external utility and partially powered by internal generation

Smart grids scheme


Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
Smart switch
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

Source: GAO analysis.

Smart grids as critical asset in port

The smart grid is a **critical asset** within the port infrastructure, so that it's a high-level target for cyber-attacks.

This increases the risk of cyberattack, where malicious software is able to take advantage of the increasing application of IT technologies

Such attacks are often based on malicious software (malware), which makes use of a **controlling entity on the network to coordinate and propagate**

The point is “INTELLIGENCE”, it provides great benefits but can be the source of great disasters when attacked and forced to operate incorrectly

Technological advances introduce new vulnerabilities and criticalities of security and require accurate verification of compatibility with technical requirements needed in the management of critical infrastructures

Smart grids as critical asset in port

A sophisticated attacker can attempt to modify the behavior of a SCADA and, in particular, directly or indirectly influence data (states, measurements, alarms) and commands (continuous and discrete) to mislead the supervision and control system.

SMART GRID VS PORT

SMART MICRO-GRID: an enabler for port competitiveness

SMART MICRO-GRID: an asset to be protected

Cyber MAR

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

WMU WORLD MARITIME UNIVERSITY

Monica Canepa, World Maritime University

✉ moc@wmu.se

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