IEEE Cyber Security & Resilience 2021
Cyber Ranges and Security Training Workshop

The Cyber-MAR Project: First Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Risk Assessment

Dr Olivier JACQ, DIATEAM

July 26th 2021, Cyberspace

Time for presentations

Dr Olivier JACQ

- Former French Navy Senior Officer, 20+ years in maritime cybersecurity
- R&D at DIATEAM and CTO at France Cyber Maritime

This paper is co-authored with:

- Pablo Giménez Salazar (Port of Valencia),
- Kamban Parasuraman (AIR Worldwide),
- Jarkko Kuusijärvi (VTT Technical Research Centre of Finland Ltd),
- Andriana Gkaniatsou, Angelos Amditis (Institute of Communication & Computer Systems),
- Evangelia Latsa (SEAbility Ltd)

Overview

- About the Cyber-MAR project

1. Port: a key infrastructure
2. Port IT and OT overview
3. Port Hybrid Cyber Range Design Methodology
4. The attack scenario
5. Benefits, Limitations and Perspectives

- Conclusion

About the Cyber-MAR project

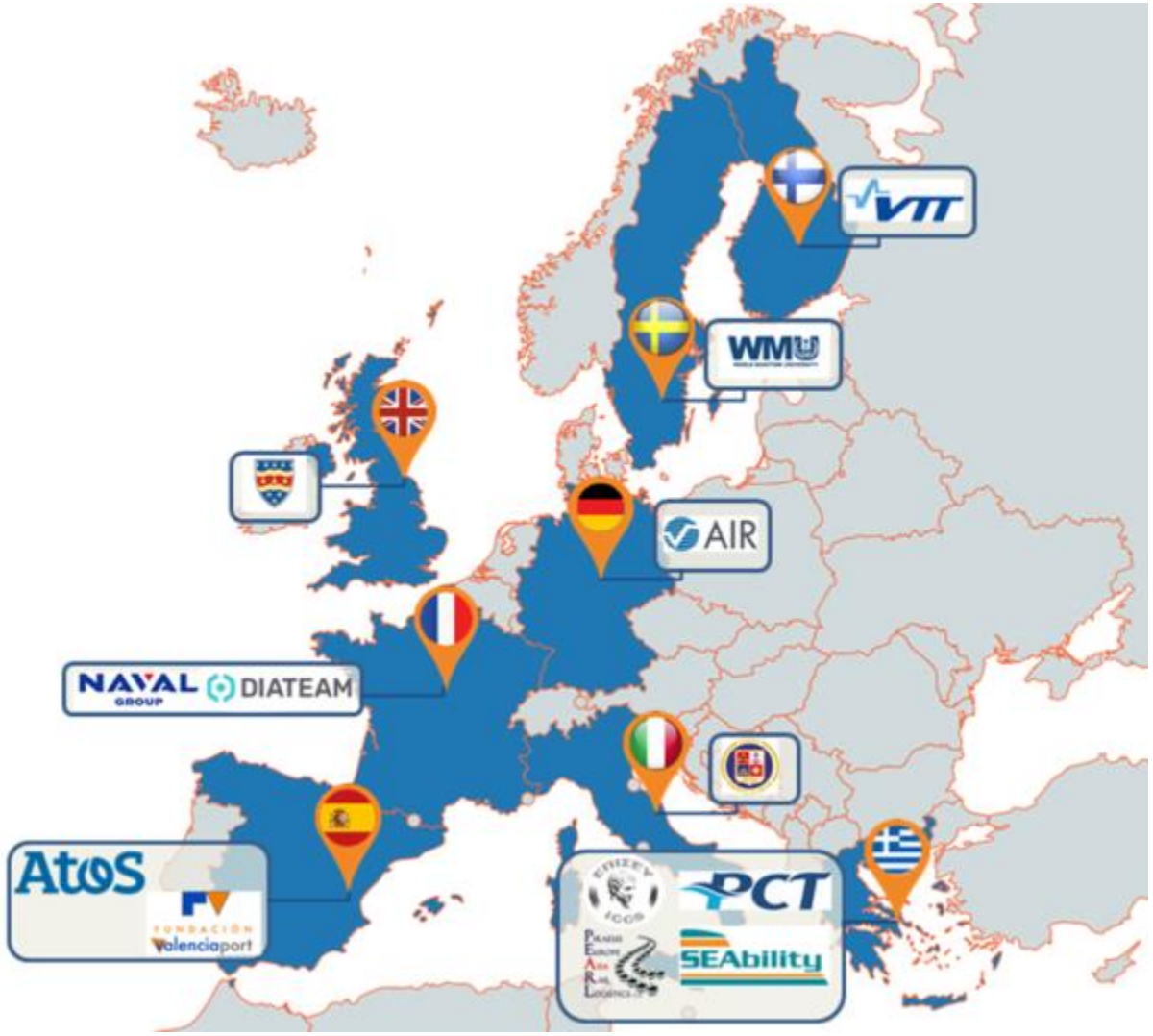
H2020 program funded by the EU

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

1. Develop innovative cybersecurity simulation environment
2. Unlock the value of use of cyber ranges in the maritime logistics value chain

The Cyber-MAR project

- 13 partners
- 8 EU countries
- 3 SMEs
- 3 industries
- 2 research organizations
- 3 universities/foundations
- 2 end users



Three pilot scenarios

1. Energy sources in the port of Valencia
2. Vessel navigation and automation systems
3. SCADA system in port container terminal

The port: key infrastructure of the supply chain

1. > 80% of goods transportation (vol)
2. Digitizing at a fast pace
3. Cyberattack could have important impact
4. Complex cybersecurity implementation
5. Need for awareness, training

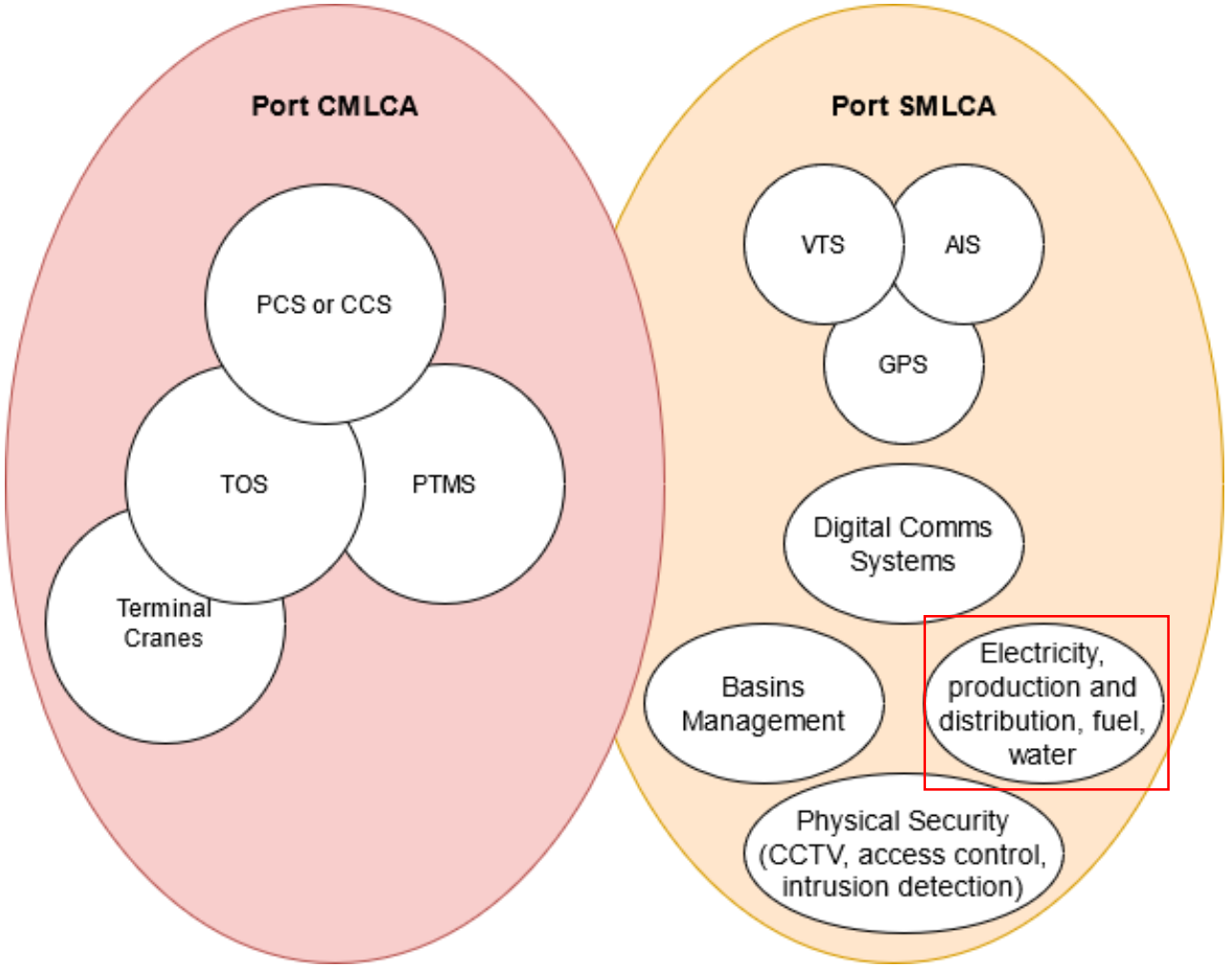
Cyber ranges are efficient tools for such needs [UKWANDU, 2020].

Maritime CR design methodology

1. Base scenarios on known cyber incidents: ADMIRAL data set
2. Need for inventory of IT/OT assets
3. Take into account maritime peculiarities
4. Use real physical assets

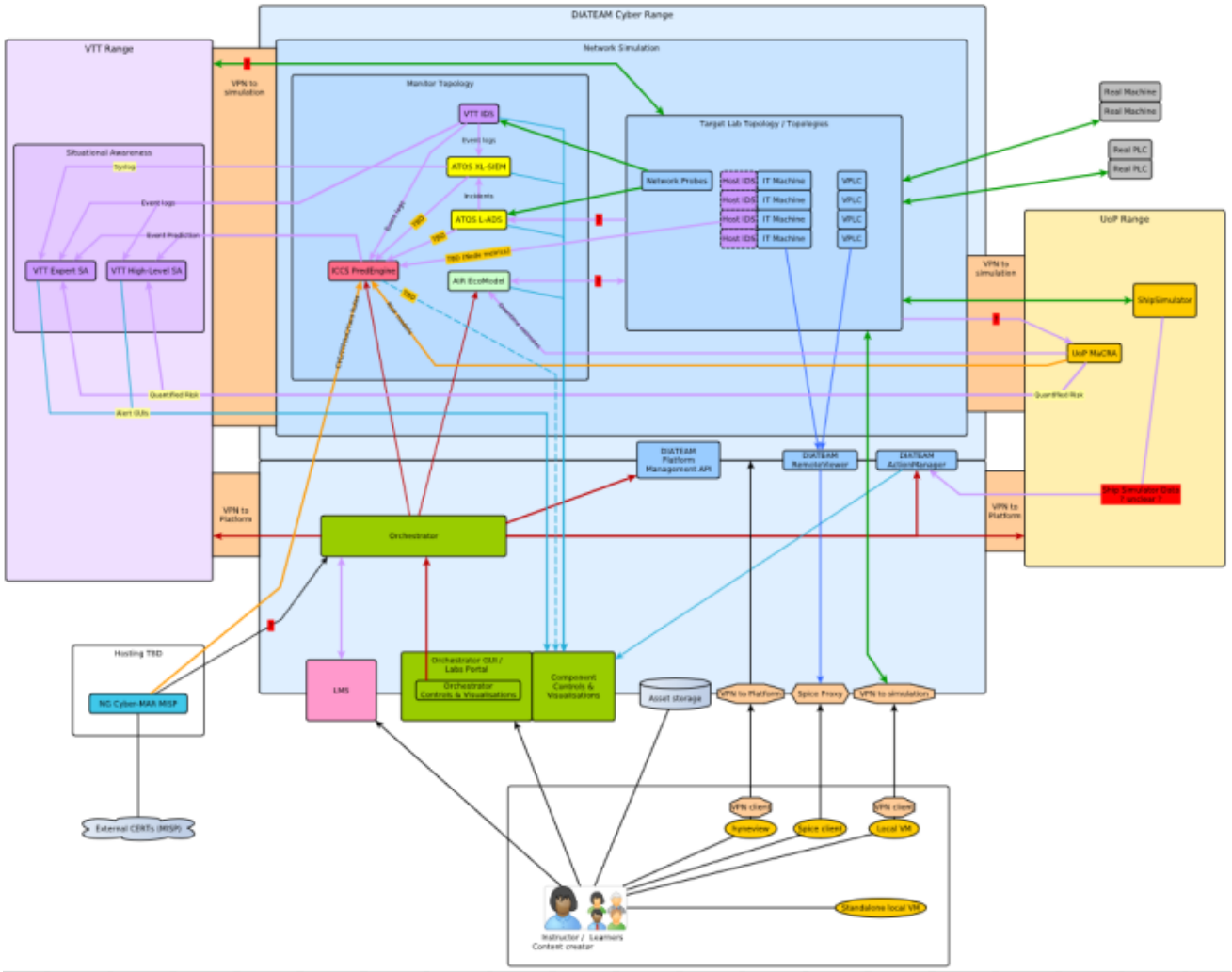
The port: mixed IT and OT systems

- Classical IT systems
- Plant-like OT/ICS systems
- Specific maritime systems
- Core and Secondary Maritime Logistics Chain Assets



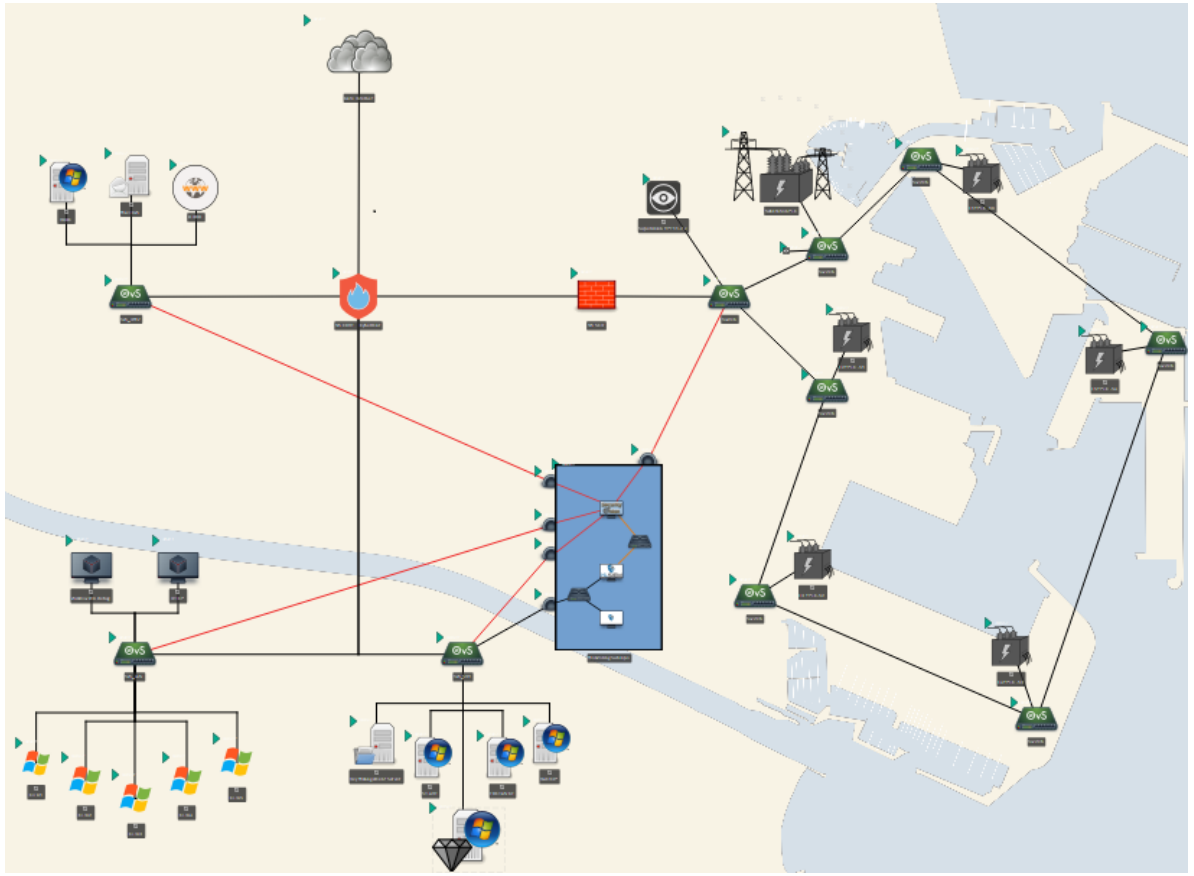
Nine layers of topology

1. Ship / Port Simulation
2. Cyber Range
3. Network Monitoring
4. Security Layer
5. CERT Layer
6. Recommendation Layer
7. Training Layer (LMS)
8. Risk Modelling Layer
9. Econometric Layer



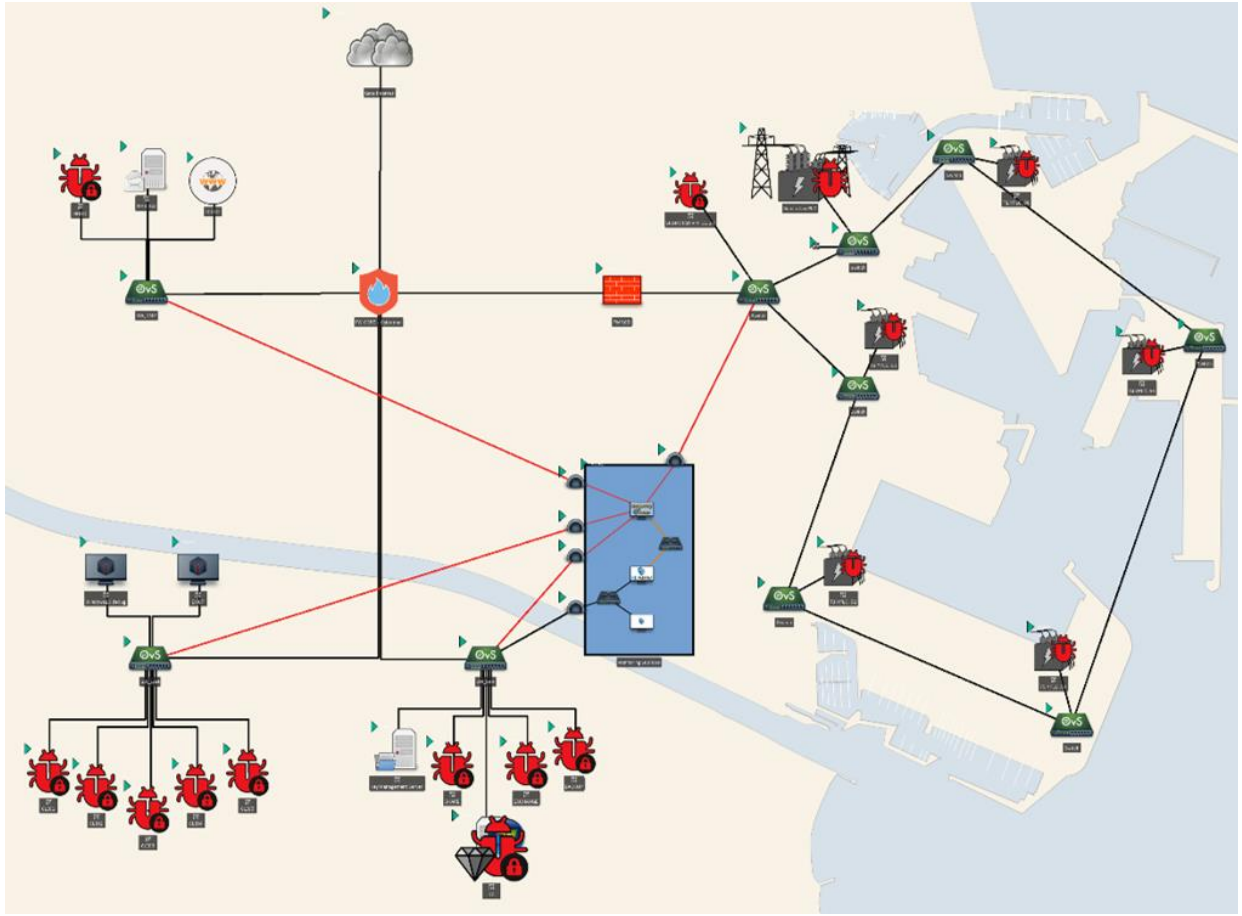
The Port of Valencia Pilot Topology

- Port Electrical Grid
- High dependency on electricity
- ICS digitalization and risks
- Simplified but realistic
- Hybrid: real PLC and ICS software, firewalls, ERP, AD, mail, backup…



The Port of Valencia Pilot Compromised Topology

- Spear phishing email
- Microsoft Office macro content enabled
- AD compromission (CVE-2020-1472)
- Lateralization on the network
- Ransomware behaviour on the whole system
- Final viral charge to the PLC
- Power outage



Benefits, Limitations, Lessons Learned

Benefits of the hybrid CR

- Cyber awareness raising for number of actors and needs
- Realistic environment for cybersecurity tooling and testing
- Data production, gathering and analysis for security and econometrics
- Patch management process
- Real added-value of the hybrid features
- Good level of detection of the cyberattack

Limitations & perspectives

- Complex and time-consuming development
- Simulation = limitation?
- Human real life traffic generation
- Need for high end red team assets
- High speed of the attack (a few minutes)
- More hybrid characteristics
- Patch management and mitigation
- Econometrics

Conclusion

1. Main objectives for the pilot port scenario achieved
2. Further data analysis is being processed
3. Two more pilot scenarios to be runned with an extensive use of the hybrid features

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

DIATEAM
MILITARY & CIVIL CYBERSECURITY SOLUTIONS

Dr Olivier JACQ, DIATEAM

olivier.jacq@diateam.net

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