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

Olivier Jacq*, Pablo Giménez Salazar†, Kamban Parasuraman‡, Jarkko Kuusijärvi§,
Andriana Gkaniatsou¶, Evangelia Latsa‖, Angelos Amditis¶
* DIATEAM
Email: olivier.jacq@diateam.net
† Fundación Valenciaport
Email: pgimenez@fundacion.valenciaport.com
‡ AIR Worldwide
Email: kparasuraman@air-worldwide.com
§ VTT Technical Research Centre of Finland Ltd
Email: jarkko.kuusijarvi@vtt.fi
¶ Institute of Communication & Computer Systems (ICCS)
Email: [andriana.gkaniatsou@iccs.gr, a.amditis@iccs.gr]
‖ SEAbility Ltd.
Email: adm@seability.eu

***Abstract*—With over 80% of goods transportation in volume carried by sea, ports are key infrastructures within the logistics value chain. To address the challenges of the globalized and competitive economy, ports are digitizing at a fast pace, evolving into smart ports. Consequently, the cyber-resilience of ports is essential to prevent possible disruptions to the economic supply chain. Over the last few years, there has been a significant increase in the number of disclosed cyber-attacks on ports. In this paper, we present the capabilities of a high-end hybrid cyber range for port cyber risks awareness and training. By describing a specific port use-case and the first results achieved, we draw perspectives for the use of cyber ranges for the training of port actors in cyber crisis management.**

***Index Terms*—cyber range, port, maritime, risk assessment, training.**

I. Introduction

The maritime sector, as many industries that heavily rely on cyber-connected systems, has been affected by the rising number of complex cyber-attacks. Generic and common attack vectors, such as phishing, infected USB devices and vulnerabilities exploited on unpatched connected systems, have been shown to cause a direct impact on critical maritime infrastructures such as ports' Information Technology (IT) and Operational Technology (OT), including Industrial Control Systems (ICS) [1]. Maritime-specific cybersecurity risk assessment has become essential, creating a growing need for raising security awareness in the maritime sector, including port operators, stakeholders, users and third parties. Cyber Ranges (CR) and Test-Beds are now recognized as efficient tools to raise cyber awareness [2] and, when they implement a realistic simulation of the ports' IT and OT infrastructures, could provide a valuable prevention measure for port cybersecurity [3]. There are more than 80 core ports in the European Union, supplying the whole economy with essential goods and raw materials. The major role of these modern and increasingly complex facilities in the supply-chain logistics has led the Cyber-MAR consortium to focus on port cyber-risk assessment and awareness. Given the complexity of ports' IT & OT infrastructures, the level of heterogeneity of the systems, and the number of system providers involved, abstracting an entire port's digital infrastructure with the use of features such as Physical to Virtual (P2V) or Digital Twin technologies is very demanding. This paper addresses the challenge that the complex maritime environment creates, and presents a first detailed CR use-case on a port cyber-attack scenario. The presented realistic hybrid CR was developed during the Cyber-MAR H2020 project, which aims to enhance port cybersecurity capabilities and the overall maritime logistics chain. The Cyber-MAR framework will also allow end-users to model and estimate the economic impact of the cyber-attack scenarios on a port, assisting organizations in properly measuring and evaluating the effect of vulnerabilities on their value chains before these disruptions unfold in real life.

Section II presents the Cyber-MAR components and the methodology used to design and conduct the pilot cyber-attack scenario on a hybrid CR. Section III describes the hybrid cyber-attack scenario designed and implemented on the CR to simulate a cyber-attack on a port. Results of the pilot use case are presented in Section IV. Section V presents the future evolution planned for the current CR to meet further research, education and operational expectations. Finally, conclusions

978-1-7281-5684-2/20/$31.00 ©2021 IEEE

are drawn in Section VI.

The main objective of the Cyber-MAR H2020 project is to develop innovative environments reproducing, as well as possible, the particularities of the maritime sector's logistic chain to allow the simulation of advanced and realistic cyber-attack scenarios, and the training of personnel to prepare for and respond to them. Cyber-MAR defines three intermediate steps in the form of pilot scenarios, to iteratively build the capabilities from different viewpoints. Two of the pilots address mainly the port environment and its surroundings, while the third one focuses on vessel IT and OT systems, and their potential impact on the logistics supply chain. Each pilot scenario is designed to be as realistic as possible, one of the objectives being to raise awareness on current and future threats for the public actors and authorities, ports operators and managers, research and education, as well as for security professionals. The integration of these scenarios within a CR is beneficial for all the actors involved. On the cyber-awareness side, the implementation aims to provide authorities and port operators with a live environment very similar to the one they use on a daily basis, rather than a generic one. As potential future users of the CR, the realism of the CR will also contribute to meeting their expectations in crisis management, intrusion detection policies and technologies, risk assessment, and mitigation strategies. The capture and demonstration of advanced cyber-attack scenarios and their cyber-physical consequences in an industrial environment raises the CR value in the educational sector. Realistic CRs also enable the production, gathering and analysis of data for security and econometric research purposes. Cybersecurity professionals benefit from such environments for multiple tasks: red, blue and purple team education and training, cybersecurity solutions testing and integration in a complex environment, secure architecture design and patch management testing to name a few.

However, designing and developing a feature-rich CR meeting these expectations is a complex and time consuming objective. In order to fulfill its ambitious goals, the Cyber-MAR project is federating experienced hybrid CR and Test-Bed partners in the design phase of the hybrid topologies, for the hosting of the complex environment with numerous virtual machines, networks and Programmable Logical Controllers (PLCs), but also high-end Red Team assets for the designing and carrying-out the attack scenarios both at the tactical and technical levels. These individual capacities, coupled with the integration of port operators, cybersecurity experts and people from the research and education fields, has led to promising first results of this multidisciplinary research work. Previously published results cover the whole project objectives [4], dedicated risk assessment frameworks for ports [5], and training and cyber-threat preparedness for logistics [6] [7].

II. Cyber-MAR approach for port risk assessment

In this section, we first describe the Cyber-MAR H2020 project, its objectives and current work in progress, as well as the methodology followed to design and conduct the pilot cyber-attack scenario on our hybrid CR.

A. Cyber-MAR components and architecture

Cyber-MAR consists of a multilayered architecture and nine layers, integrating the different components addressing the CR capacities. Each layer is implemented by the corresponding modules, listed below:

- *Ship simulation layer*: the ship simulation module provides a realistic environment of an operational ship and the traffic between its different components.
- *Cyber Range (CR) layer*: using virtualization, task automation and orchestration, virtualized networking and hybrid connection to real PLCs and other equipment, the CR module offers the underlying environment for training and prototyping topologies consisting of networks and systems.
- *Network Monitoring layer*: the CR topologies are monitored by Intrusion Detection System (IDS) and Situational Awareness (SA) tools. The IDS is responsible for analyzing the network traffic and detecting suspicious behavior and potential attacks. The module identifies traffic patterns and compares them to the existing rules that model potential threats. The IDS uses both publicly available (eg. Emerging Threats) and scenario-specific rules using Indicator of Compromise data (IoC) from the Malware Information Sharing Platform (MISP) deployed in the CR. Through dissection, analysis and monitoring of the network traffic, a situational awareness visualization of the current situation is constructed. SA provides multiple views of the data, in which the separate viewpoints to the data can be defined, or different detailed data can be visualized depending on the user's needs.
- *Security Layer*: the Security Information and Even Management (SIEM) and Anomaly Detection System (ADS) modules implement the security layer. The SIEM module provides a security analytics platform enhanced with a high-performance correlation engine to deal with large volumes of data, and can provide scalability by distributing the processing of security events across multiple nodes. It raises security alerts from a business perspective based on events collected from different data sources at different layers of Cyber-MAR. The ADS module provides live anomaly detection, analyzing network traffic and NetFlow data using unsupervised machine learning to identify anomalous behaviors in device communications.
- *Computer Emergency Response Team (CERT) Layer*: the CERT module is based on technical and operational data such as Tactics, Techniques and Procedures (TTP) and IoCs produced by inter-CERT cooperation. The module is responsible for enhancing the knowledge stored in the MISP cybersecurity cooperation platform by setting up and taking part in a MISP community dedicated to the maritime sector stakeholders. In this community, over 500 generic and maritime-specific IoCs and cybersecurity threats were shared and implemented to improve cybersecurity preparedness and provide early warnings.
- *Recommendation Layer*: the recommendation module

provides a machine learning based analysis of the detected attacks, and uses a Variable Length Markov Model (VLMM) to project the potential future IDS/SIEM alerts and consequently the next threats.

- *Training layer*: the Learning Management System (LMS) module aims to improve the performance and the experience of the training. The module will provide the course catalogue of the training, the complete courses, the assessments, and the specific assignments. It also allows monitoring and management of certification and retraining activities (eg., management of recurrent training, continuous updates, compliance programs *etc.*). Training activities will be assigned individually, or according to the specific role of the trainee within the organizational structure.
- *Risk Modelling Layer*: the Maritime Cyber-Risk Assessment (MaCRA) module measures the level of cyber-risk exposure of the target systems. A risk model is then applied to a discrete event simulation model of the port operations so that an estimate of the expected effect of cyber-attacks on the maritime operations can be calculated.
- *Econometric Modelling Layer*: the econometric modelling module translates the port downtimes estimates for different cyber-attack scenarios to an equivalent measure of financial losses for different nodes in the value chain.

B. Methodology

In this section, we describe the process we followed to design the pilot event for the first port scenario on the project's CR. As recommended by the NIST and other similar frameworks, the first step involved individual identification tasks. First, we identified and compiled past disclosed cyber incidents which affected ports. Then, we produced an analysis of the ports' IT and OT systems. Finally, based on our analysis and findings, we produced a realistic scenario and topology for the CR.

1) Public cyber impacts on ports: Maritime cybersecurity has attracted a lot of attention in research, with a rising number of findings. However, the area lacks a common, comprehensive and regularly updated dataset of disclosed maritime cyber incidents. During the Cyber-MAR project, a dataset containing over 90 disclosed incidents for the maritime sector from 1998 to 2021 was generated and released [8], making it publicly available for the research community. The public can access, contribute, and create merge requests to update, maintain and enhance this database. The number and type of incidents and variety of sources contributed to the enhancement of the port cyber-attack scenario.

2) Port information systems identification and classification: The first step during the design phase is the identification of the port IT and OT assets. However, all ports are different, regarding either their specialty (*e.g.* passengers, containers, bulk...) or role in supply chains, but also their size and their network and software architecture. Therefore, defining and modeling a common architecture (or topology) for ports on the CR is a difficult task. For this reason, we decided to start by defining generic port functions before digging into the underlying information systems. The first identified function of a port is the possibility to communicate within the port and with other partners by various means, in order to ensure the proper working of the processes and logistics, security and safety chains among all actors. The second function aims to guarantee port's safety and security, to comply with International Ship and Port Facility Security (ISPS) and other international or national regulations. The third function is to ensure a safe and secure cargo delivery in and out of ships, for instance through the use of tracking tools, devices and cranes. The fourth function isolated concerns the management, operation, and monitoring of port assets (*e.g.* basins, pumping, doors, locks, and gates). Finally, the port authority is also in charge of providing support for the ships (*e.g.* communications, power supply, crew, bilge, tugs, electricity, fuel, and water), and responsible for port planning, coordination and maintenance on short-, mid- and long-term periods.

Identifying generic port functions helps determining IT and OT systems that are present in most medium to large size ports. Port Community System (PCS) and Cargo Community System (CCS) are the common data hubs for all actors involved in a port, respectively regarding ships and cargo management. With their central role, any disturbance in the operation of PCS and CCS could lead to major havoc in large ports with tremendous negative effects to maritime supply chains and the economy [9]. The Terminal Operating System (TOS) or Port Terminal Management System (PTMS) are systems mainly used for container terminal management (both for logistics and terminal crane management) [10]. Vessel Traffic Service (VTS), Automatic Identification System (AIS), and Global Navigation Satellite System (GNSS) - such as GPS - are widely used in ports, for instance to follow ships' and tugs' activities and even for crane management. Digital Communication Systems (*e.g.* 4G, 5G, trunking radios, WiFi, WiMax), as well as classical phone systems or VoIP/ToIP, are used for coordination, safety, and security. The physical security of ports relies on systems such as Closed Circuit Television (CCTV), access control systems for passengers and trucks, and physical intrusion detection systems. Finally, depending on the size and automation level, the port may also use a large number of ICS for basin management (*e.g.* pumping stations, locks), electricity production and distribution, and fuel and water distribution, that all directly contribute to their operations [11]. Depending on the type of a port, IT and OT will have various functional (*e.g.* network, Active Directory) and physical (*e.g.* electricity, data center) dependencies. Such a variety of IT and cyber-physical systems makes it difficult to construct a global situational awareness [12].

The IT and OT systems involved in the maritime logistics value chain for ports can be classified in two groups: Core Maritime Logistics Chain Assets (CMLCA) and Secondary Maritime Logistics Chain Assets (SMLCA) (Fig. 1). CMLCA are the IT/OT systems operating the logistic chain, while SMLCA are the systems without which CMLCA would not be able to function. Even though SMLCA are not strictly part of the logistic supply chain, their contribution to it is essential. Threats, risks and vulnerabilities for CMLCA and SMLCA may also be specific, and there is a real need to understand dependencies between them and the possibility of the spread of an attack or cascading failure across these systems. The risk of a cyber-attack propagation between ship and port also has to be taken into account. CMLCA, such as PCS/CCS, TOS, PTMS, and terminal cranes are essential assets for the logistic value chain. In large ports, there is however no easy way to mitigate a PCS/CCS/TOS or PTMS failure, as the potential backup solutions (*e.g.* paperwork, manual email or social networks, cargo delivery alternatives) cannot cope with the fast pace of port activities. For SMLCA, VTS, AIS and GNSS systems are the most important for surface situational awareness. However, in most cases and weather permitting, port authority keep a visual watch on ships in the vicinity, therefore, human presence can be considered as a resilience measure. Digital Communications Systems are an important means to ensure proper communication between port actors and external actors. Nevertheless, backup communication solutions should be available. Industrial Control Systems disruptions - *e.g.* in basins management or fuel and water distribution - may have a significant impact on CMLCA. Often, manual backup solutions can minimize this impact on the logistic chain. However, electricity production and distribution remain essential for all CMLCA and SMLCA assets and port operations.

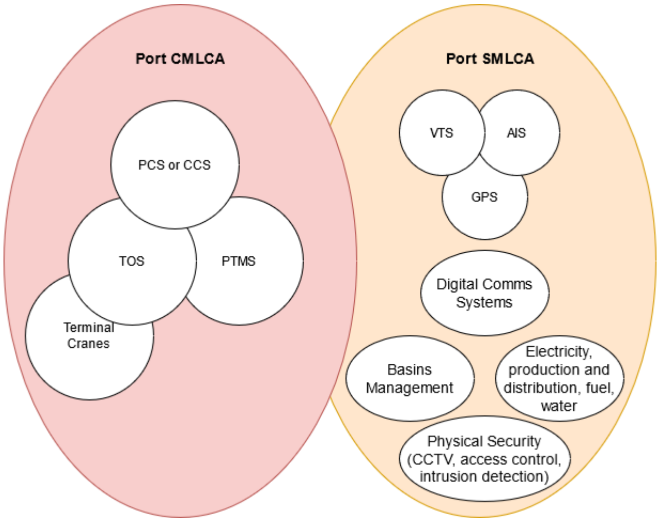
Port CMLCA
PCS or CCS
TOS
PTMS
Terminal Cranes
Port SMLCA
VTS
AIS
GPS
Digital Comms Systems
Basins Management
Electricity, production and distribution, fuel, water
Physical Security (CCTV, access control, intrusion detection)

Fig. 1. CMLCA and SMLCA systems for ports.

III. Port cyber-attack scenario on a hybrid cyber range

Our work in CMLCA and SMLCA definition underlined that generic port functions strongly rely on IT and OT systems to operate. This led to three major scenario inputs for the definition of our first scenario. Firstly, all IT and OT systems depend on electricity to operate, and even with backup solutions, a significant electricity disruption would have serious consequences on port operations. Secondly, the ICSs used for energy production and distribution are also digitized and might be connected to the port network, presenting a potentially wide attack surface. Thirdly, as port processes strongly depend on electricity – from traffic guidance systems to cargo transportation - a cyber-attack targeting the port's electrical grid system could have a huge impact. For instance, in the port of Valencia, a lot of companies have their premises inside the port area (*e.g.* terminals, shipping agencies, haulier companies, freight forwarders, nautical technical services, and security organizations). Some of these companies have high energy needs, such as the container terminals. The port authority has the energy provider role within the port, providing power to all these companies. These inputs logically led to the choice of modeling a CR topology and attack scenario targeting the electrical grid of a port. After conducting a thorough analysis on these assets with port operators, we extracted their specifications and incorporated them into the CR port pilot topology.

The electrical grid architecture defined for the first pilot is a simplified, yet realistic, model based on the actual infrastructure in the port of Valencia. It contains the part of the industrial networks - such as PLCs and industrial switches - providing power to all the systems, sensors, infrastructures, and companies in the port premises. It is composed of a network ring connecting six transformer stations distributed inside the port. The head station supplies power to the other stations, which provide power to the elements described above; at each station, a PLC is used to manage the transformer and measure consumption. The hybrid technology capacity on the CR enabled us to use a real physical PLC for the head station, while the others were simulated, acting and communicating in a realistic manner. An ICS supervision dashboard was built to monitor and interact with the PLCs. The architecture also contains the usual IT systems and servers used by a real port authority, such as firewalls, Enterprise Resource Planning (ERP) and Active Directory (AD) services, mail and backup servers, personnel workstations, etc. The OT systems and supervision workstation were set up in a separate network segment without Internet access, firewalled from the main port IT systems, but joined to the same domain. The CR topology also includes the necessary Cyber-MAR components described in Section II-A, and a simulated ”Internet” network. The main actor in the demonstration is the port authority OT manager, who has access to the SCADA supervision system from his workstation.

IV. Results and discussion

For the first pilot demonstration, we deployed the topology presented in Section III on the Cyber-MAR hybrid CR and performed live cyber-attacks according to the scenario. During this real-time demonstration, the port authority OT manager receives a spear-phishing email from an attacker with a malicious attached document. The initial infection vector is triggered when the user enables the macro content in the document: the malware automatically installs itself persis-

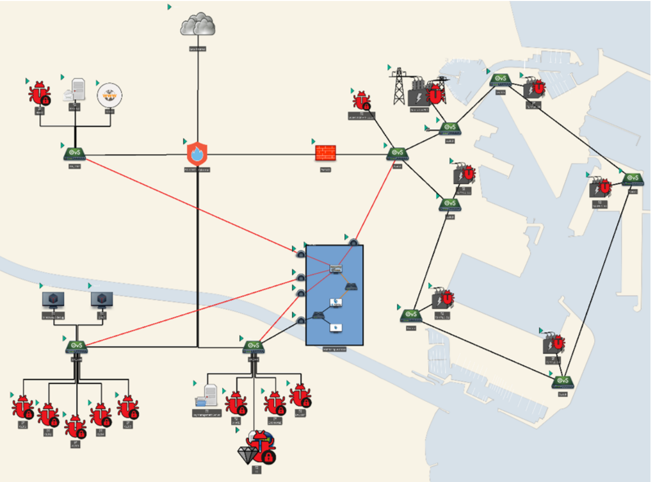

Fig. 2. The CR pilot topology, once compromised by the viral charge.

tently. The malware checks the membership of the infected workstation within an Active Directory domain and obtains the address of the AD domain controller. Taking advantage of a simulated poor patch management process, the malware exploits the Zero-logon vulnerability (CVE-2020-1472) to gain administrator rights on the AD server. With this access, the malware can perform lateralization through the network, infecting the AD server by abusing the SMB protocol, and installing itself persistently. Running as administrator on the AD server, it can copy and execute itself on all systems in the the domain using Windows Remote Management (WinRm), and setup permanent reinfection via Group Policy Object. As the malware propagates throughout the network, it executes on each infected system, including the AD server, to encrypt all files with a ransomware module, so that the port users cannot access their files or systems until paying for the decryption key, or restoring from (often incomplete) backups. On each infected machine, the malware also searches for SCADA management software to trigger its main viral charge. The malware searches for the PLCs' addresses, uses the Modbus protocol to access the PLCs and sends commands to stop them (via Modicon STOP on the physical PLC). The real PLC is then reflashed with a compromised program. As a result of the cyber-attack, a power outage throughout the port is caused. This kind of attack could also potentially cause physical damage to the power distribution infrastructure or downstream equipment. Fig. 2 presents the compromised simulated infrastructure. During these different phases, over 570k network packets were transmitted over the CR. Throughout the demonstration, the three Cyber-MAR detection components deployed in the CR (IDS, SIEM and SA) followed each stage of the progression of the malware, with 10 signatures identifying the attack. This pilot demonstrated that the performed attacks could be detected with relevant and properly configured tools monitoring the traffic of the IT and OT networks. Moreover, the pilot event gave the participants an idea on how a cyber-attack might progress in a real system. Finally, the alert to a dedicated maritime CERT can enable the analysis and sharing of the attack details (Tactics, Techniques, & Procedures and IoCs) in order to warn other potential victims in the maritime sector.

Following the live demonstration experience, an evaluation phase was set up by the consortium through an online survey to check how the pilot and the results achieved on the hybrid CR had met the objectives of the Cyber-MAR project detailed in Section I. The CR pilot had very positive feedback on interest, motivation and awareness raising. Assessments that would have required hands-on testing, like familiarisation with the system or ease of use had more uncertainties. For future pilots, processes for halting or preventing the attack were seen as interesting and, on the other hand, the demonstration was commented to be perhaps too technical for the non-technical participants. The involvement of a port authority during all the phases of scenario greatly enhanced the realism of the topology. Even if, as expected, the whole port network and software architecture virtualization could not be implemented, the SMLCA represented by the electricity production ICS, the numerous IT systems seen in Fig. 2 and the hybrid features of the CR were highly realistic, meeting the expectations relative to awareness raising on current and future threats for the port actors but also for educational use. The cyber sensors deployed enabled the collection of a large amount of data to be analyzed by cybersecurity and econometric researchers. Finally, the hybrid CR proved to be a valuable environment for cybersecurity professionals to test their product integration and configuration in the complex environment of a port.

V. Perspectives for the Cyber-MAR cyber range

In the global economic value chain, ports can be thought of as nodes of risk aggregation. A disruption to a port's operations can constrain the flow of goods, which are critical for manufacturing different products, manifesting as losses across many industries [13]. The econometric model proposed in Cyber-MAR is a quantitative risk model that emulates major components of the global supply chain and calculates a mean contingent business interruption (as a downtime measured in days), with a range that accounts for the uncertainties inherent in risk modelling. The proposed modelling framework can be used for developing Business Continuity Plans (BCP) for disruptions stemming from cyber-attacks on ports. The framework consists of five modules: product dependency, network definition, hazard and impact calculation, impact propagation, and loss calculation. The definition of the supply chain is based on the enumeration and the interconnection of physical parts, such as the basic and intermediate materials required to construct a final product. The next step is assessing the global trade flows of these parts among suppliers and the import and export patterns among countries. Once the conditions and assumptions for the global supply network have been established, the third step involves calculating the disruption resulting from a cyber scenario. Given the various uncertainties associated with scaling up a cyber-attack from component-level vulnerabilities and aggregating them into an equivalent downtime at the port level, a mean μ and sigma σ for this initial disruption is estimated. For the port scenario, the initial seed disruption in days is applied at appropriate root nodes (ports) of the supply chain network and then propagated and quantified at the next nodes of the chain. After all potential disruptions are calculated for each node, the losses for the final product nodes are quantified as a contingent business interruption. The final step is calculating the economic loss at target nodes of interest. This node of interest would be chosen by the end user of the Cyber-MAR platform, along with the pre-defined attack event from a catalogue of scenarios with specific attributes. The econometric model would then incorporate the attributes of the cyber scenario with the port-level vulnerability estimates from the MaCRA framework to determine the economic losses for the target node of interest and giving the end-user a visualization the quantified results with the mean μ and sigma σ of the economic loss estimate. Regarding the distribution that is used to represent the economic loss estimate, the magnitude of the uncertainties will control the shape of the curve. A shallower curve would have a greater sigma σ and depict larger uncertainties for a scenario. By using a range of loss estimates, the framework informs the end user as to the possible magnitudes of losses. The end user could then take these results and formulate a BCP plan for mitigating risk from cyber disruptions based on econometric figures and business priorities.

The CR enhancement will continue in the future, even if the Cyber-MAR project will focus on other assets of the maritime logistics supply chain. The integration of other port or ship IT/OT systems to the CR will enable live and more comprehensive ships/ports environments and even more complex interactions during cyber-attacks, enabling the necessary cooperation between OT and IT third-party maintainers and operators. This work will also include a deeper focus on patch management issues on OT systems: while patch management is an essential prevention and mitigation method, its implementation on OT systems is still a challenge, due to the potential risks for the ICS (regression, cyber-physical issues). The use of a hybrid CR on which sensors, actuators, PLCs and software can be implemented and tested to ensure no regressions are introduced seems an important experimentation path. Finally, the next steps of the Cyber-MAR project will also include the integration of the LMS and of an orchestrator to ease and automate scenario setup and interactions between learners, trainers, port actors, and the CR.

VI. Conclusion

The demonstration event set in December 2020 was a great opportunity to highlight cyber threats, risks, consequences and solutions in port critical infrastructure. After a long and intense preparation period, all objectives were fulfilled, and the benefits of the Cyber-MAR project to prevent such kind of attacks were clearly underlined. The Cyber-MAR CR allowed us to design and deploy the topology of a port's IT and OT critical infrastructure with real cyber-physical systems and devices. It can be used to simulate a wide range of cyber-attacks with three main objectives: detect attacks, mitigate risks and train personnel to act in such crisis situations. The pilot demonstration also highlighted to the participants that, although the different Cyber-MAR components were able to detect the attack, the pace of the attack was too fast to stop it once the attacker gained administrative access to the organization's network. That is why dynamic prevention and reaction measures are essential to avoid the initial attack vector and prevent the spreading across the network infrastructure. The topology now seems mature enough to help with the training of port employees, stakeholders and third parties to enhance awareness and mitigate risks.

Acknowledgments

This paper is part of the research efforts under the Cyber-MAR project, which has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 833389. Content reflects only the authors' views, and the European Commission is not responsible for any use that may be made of the information it contains. The authors would like to thank all participants of the Cyber-MAR H2020 project for their continuous and rich involvement in the specification and realization of this port CR use-case.

References

[1] Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554.

[2] Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. (2020). A review of cyber ranges and test-beds: current and future trends. Sensors, 20(24), 7148.

[3] Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. The Asian Journal of Shipping and Logistics, 37(1), 20-36.

[4] Tam, K., Moara-Nkwe, K., & Jones, K. (2021). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. Maritime Technology and Research, 3(1): 16-30.

[5] Tam, K., Moara-Nkwe, K., & Jones, K. (2021). A Conceptual Cyber-Risk Assessment of Port Infastructure.

[6] Pyykkö, H., Kuusijärvi, J., Silverajan, B., & Hinkka, V. (2020). The Cyber Threat Preparedness in the Maritime Logistics Industry. Proceedings of 8th Transport Research Arena, 27-30.

[7] Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021, March). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. In Proceedings of INTED2021 Conference (Vol. 8, p. 9th).

[8] Jacq, O. Advanced Database of Maritime cyber Incidents Released for Litterature, ADMIRAL repository, retrieved from https://gitlab.com/m-cert/admiral

[9] Meyer-Larsen, N., & Müller, R. (2018, February). Enhancing the cybersecurity of port community systems. In International Conference on Dynamics in Logistics (pp. 318-323). Springer, Cham.

[10] Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. Computers & Security, 103, 102196.

[11] Kosmowski, K., & Gołębiewski, D. (2019). Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. In Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars (Vol. 10, pp. 99-126).

[12] Adams, N. P. H., Chisnall, R. J., Pickering, C., & Schauer, S. (2020). How port security has to evolve to address the cyber-physical security threat: lessons from the SAURON project. International Journal of Transport Development and Integration, 4(1), 29-41.

[13] König, S., Rass, S., & Schauer, S. (2019). Cyber-attack impact estimation for a port. In Digital Transformation in Maritime and City Logistics: Smart Solutions for Logistics. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 28 (pp. 164-183). Berlin: epubli GmbH.