Monica Canepa
World Maritime University (WMU)
moc@wmu.se
Fabio Ballini
World Maritime University (WMU)
fb@wmu.se
Amditis Angelos
I-SENSE group / Institute of Communication and Computer Systems
a.amditis@iccs.gr
Baroutas George
I-SENSE group / Institute of Communication and Computer Systems
george.baroutas@iccs.gr
Sdongos Evangelos
I-SENSE group / Institute of Communication and Computer Systems
evangelos.sdongos@iccs.gr
Dimitrios Dalaklis
World Maritime University (WMU)
dd@wmu.se
Vasiliki Palla
Seability
vasiliki.palla@seability.eu
Elena Krikigianni
Seability
e.krikigianni@seability.eu
Evangelia Latsa
Seability
adm@seability.eu
Seyedvahid Vakili
World Maritime University (WMU)
W1701221@wmu.se

Cyber-security training platform on realistic maritime logistics scenarios

Extended Abstract (max. 1200 words)

Objective (max. 300 words)

The maritime sector remains one of the most important financial sectors for the European economy. Acting as the backbone of world trade, around 80% of world trade in goods is carried by the

international shipping industry domain and is in full growth[1]. The growing digitization in the maritime logistics domain is one of the driving factors towards its growth. However, the growing digitization of the maritime value chain actors increases the attack surface of maritime information systems. Maritime information systems, whether on board of ships or in ports, are numerous, built with standard components available on the market and in many cases designed without accounting for the cyber risk, which is ever growing. Despite the fact that cyber risk management is encouraged to be followed by competent authorities**2**, there is still large room for improvement. The importance of handling cyber preparedness as a highly prioritized aspect is paramount.

The lack of awareness about cyber threats is evident in several different business sectors, including the maritime sector. While there have been relatively few announced reports of successful cyber-attacks on either shipping or on shore-based facilities, they had considerable impact and connected industries have suffered attacks suggesting that the maritime sector may be vulnerable. Its major financial contribution at European level makes the necessity to mitigate the potential cyber risks in it even more important. Two two most known cases of cyber-attacks with devastating financial and societal impacts in this domain are:

The Maersk Case: In June 2017, the NotPetya malware, hit shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks. According to a statement issued by the company, the total cost for dealing with the outbreak landed somewhere in the $200 to $300 million range

The Antwerp Port Case: Hackers working with a drug smuggling gang infiltrated the computerized cargo tracking system of the Port of Antwerp to identify the shipping containers in which consignments of drugs had been hidden. The gang then drove the containers from the port, retrieved the drugs, and covered their tracks. The criminal activity continued for a two-year period from June 2011, until it was stopped by joint action by Belgium and Dutch police.

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 cybersecurity investment plan, maritime logistics actors need to base their cybersecurity strategy on a palette of innovations, novel combinations of them and changes of mindset. In the present paper, **the proposal is related to the use of a federated Cyber Range solution being part of a cybersecurity training platform dedicated to the maritime sector specificities**. Such a platform, based on innovative technologies and their combinations will increase the cyber-awareness level and will ensure the business continuity of all involved actors. Equally important, such a platform will act as a cost-efficient training solution covering the maritime logistics value chain.

Data/Methodology (max. 300 words)

The proposed cybersecurity training platform adopts a three-tiered approach in procedures, people and technologies, following the advantages of cyber ranges. Despite the existence of various cyber ranges definitions, in the current paper we define a cyber range as "a platform for the development, delivery and use of interactive simulation environments"**3**.

[1] https://www.ecsa.eu/policy-priorities/shipping-and-trade-policy/shipping-and-global-trade
[2] GUIDELINES ON MARITIME CYBER RISK MANAGEMENT, MSC-FAL. 1/Circ. 3, IMO, July 2017
[3] Understanding Cyber Ranges: From Hype to Reality, ECSO, March 2020

The abovementioned tiers facilitate the extraction of valuable results with respect to cybersecurity in all critical aspects:

Train people: Cyber security professionals and employees in other key-areas either directly or indirectly connected with cybersecurity need to receive continuous training to be well prepared when an attack occurs.

Test technologies: Such a platform offers the opportunity to test technologies in a secure environment. Apart from its training role, the tool can act as a virtual testbed of novel technologies prior to their introduction in production.

Measure procedures: By deploying a novel cyber range-based platform possible areas for improvement in established procedures can be extracted in a realistic, cost and time-efficient efficient manner without the risk of business disruption.

The main components of the proposed platform are the following ones:

Federated cyber ranges: This comprises all the technologies, tools and methodologies (hybrid coupling, IDS/IPS, data analytics and intelligence extraction, networking with all cyber ranges, situational awareness) related to the simulation environment.

Risk analysis models: **It will implement vulnerability analysis and use risk analysis models in various potential cyber-attack.** Risk assessment component will assess ship/port or other maritime's stakeholders cyber-risks exposure by evaluating threats. This module will be integrated within the platform serving as the risk model component of the system.

Econometric Models: The econometric model will allow insurance companies and corporations assess the impact of cyber-attacks across different product groups and industries. The output metrics from the model will help organizations to quantify supply chain risk, develop risk mitigation strategies, and improve resiliency.

Results/Findings (max. 300 words)

The proposed platform in the present paper is under development4. However, the expected main results are the following:

Ensure that cyber-security and IT professionals can easily create scenarios of cyber-attacks (past or recently emerging) and/or insert data and logs from historical, current or fictional cyber-attack incidents in a straightforward manner.

Easy integration to low-level parts of the port and shipping systems (down at the level of sensors or PLCs), thus the actual effect on the real and operating environment may be estimated. More importantly, given that one of the main features of such a platform will be its interoperability of different cyber-

[4] Research activities related with the realisation of such a cyber range-based training platform are ongoing under project Cyber-MAR funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.

range systems, professionals will have the opportunity to detect attacks on collaborating organisations' systems and thus be able to fail-safe their own, not allowing for cascading effects to take place.

In the long term, better preparation derives largely from better trained, more qualified and experienced professionals. This will be made possible by the creation of intuitive scenarios of the platform and the potential for data entry from a wide range of cyber attack cases, with a variety of incidents with which they can be trained.

The econometric model developed would be first of its kind risk assessment framework for quantifying the impact from cyber-attack of the maritime domain. The quantitative metrics from the econometric model can be ingested by corporations or governmental organizations to evaluate their potential risk and optimize their risk mitigation strategies. In the long term, the econometric modelling framework would help build cyber resilience and close the protection gap that presently exists in the cyber/supply chain insurance space. In the future specific research could be dedicated to the technical and process interoperability of the Cyber-MAR platform in the world maritime industry.

Implications for Research/Policy (max. 300 words)

As previously mentioned [2] the cybersecurity policy and regulatory framework in the maritime domain is expanding. The main implications of the current research is the identification of the main gaps in maritime cyber security coupled with the training and awareness needs on cyber security aspects. What is even more evident, is the importance of handling cyber preparedness as a highly prioritized aspect on the overall governance agenda. As mentioned in various reports on cyber preparedness "There's no substitute for preparedness".

Keywords: *business continuity, maritime cyber security, cyber range, cyber awareness*