Cyber-security training platform on realistic maritime logistics scenarios

Monica Canepa
Fabio Ballini
Dimitrios Dalaklis
Seyedvahid Vakili
Luis Miguel Colmenares Hernandez

WORLD MARITIME UNIVERSITY

INTRODUCTION

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 .

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.

WORLD MARITIME UNIVERSITY

INTRODUCTION

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.

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.

Cybersecurity skill shortage

- "Digitalization phenomenon" and maritime autonomous surface ships (MASS) leads to transforming in shipping industry.

- The industry should be concerned with the cyber-security threat, since there is already a heavy reliance on electronics and software/IT applications.

- Demand for cybersecurity job positions has increased.

> "***Cybersecurity demand is twice as great as supply***".

WORLD MARITIME UNIVERSITY

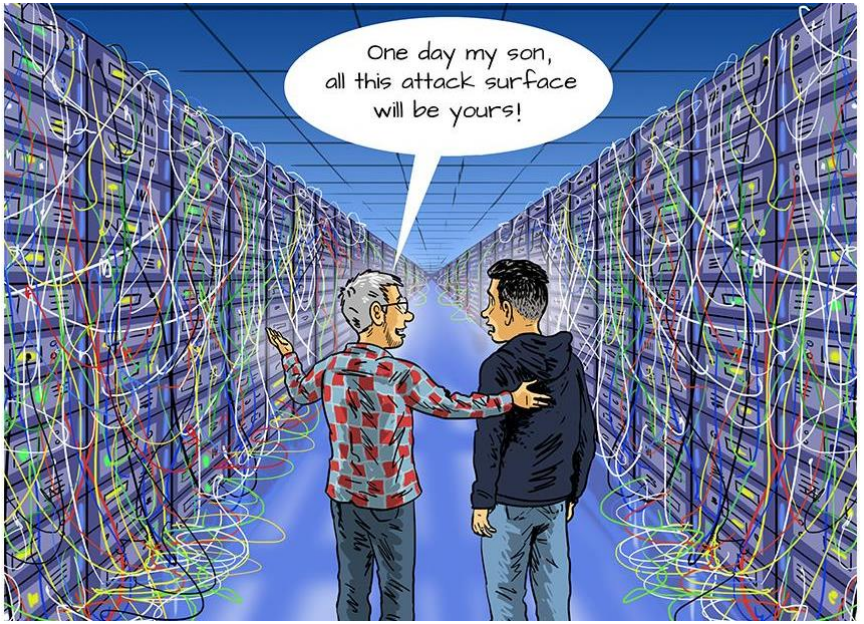
Challenges in Cybersecurity education and training

- Specialized domain.
- Very fast pace of change associated with it.
- Gaps between real requirements and academic offerings.
- Technology evolves with a high speed.
- Cybersecurity training offerings must be continuous and dynamic.
- It must be considered as a matter of public, private, social, and educational interest.
- Cybersecurity issues related education and training activities should take into account simultaneously technical, social, and legal aspects.
- Cybersecurity is the difference in how they are conducted from one country to another.
- Stakeholders have not reached consensus on cybersecurity training.

WORLD MARITIME UNIVERSITY

An interdisciplinary /multidisciplinary approach for Cybersecurity education

- Professionals involved in the specific domain have a background spanning into various different disciplines.



- These teams size should vary, depending on the “targeted mission” and must be adapted to a particular need or activity.

WORLD MARITIME UNIVERSITY

The EU Digital and Cybersecurity Education Policy

- The European Union (EU) developed the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, in 2013.

- Compulsory to raise the levels of cybersecurity awareness and the relating skills development as a priority at national and European areas (De Zan and Di Franco, 2019).

- in 2017, via joint communication to the EU Parliament and the Council "Resilience, deterrence and defence: Building strong cybersecurity for the EU"

- In the respective Digital Education Action Plan (2021 - 2027) promote:
- improving digital skills and competences for the digital transformation
- development **advanced digital skills** which produce more digital specialists and also ensure that **girls and young women** are equally represented in digital studies and careers

INTRODUCTION

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.

WORLD MARITIME UNIVERSITY

OBJECTIVES

The aim of the research is to **propose 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

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”.

WORLD MARITIME UNIVERSITY

METHODOLOGY

The above mentioned 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.

WORLD MARITIME UNIVERSITY

METHODOLOGY

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.

WORLD MARITIME UNIVERSITY

Cyber-MAR training platform

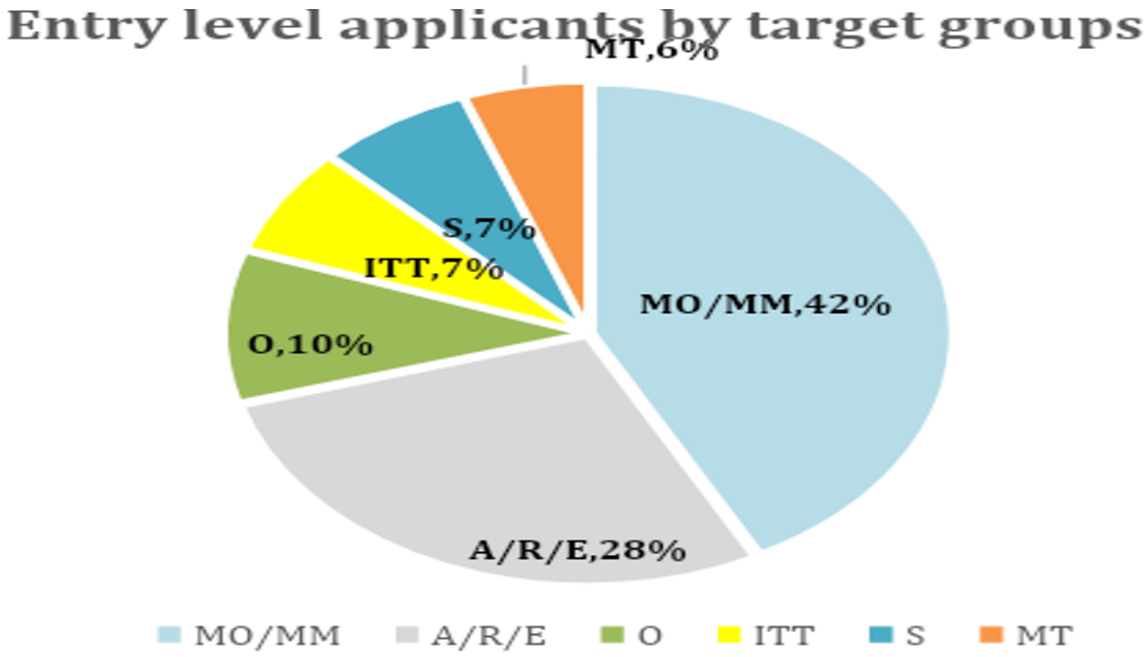
Complexity level	Details	Requirements	General aims
Entry level	Entry-level users who are not familiar with cyber security **Theoretical**	Basic skills about TCP/Ip and/or network security in reality, nothing officially required since the training will take them into that space for the first time and will be used to grant access to the second level	Training is a basic introduction to cyber security and the concept of Cyber-MAR. The goal is to raise awareness among identified users (very large audience). To give the participant the opportunity to understand cyber security threats and the basic concepts for reducing risk in the maritime sector.
Mid-level	Users who are familiar with cyber security and wish to increase their skills to a higher level **Theoretical and hands on**	Middle level : it's a must that they have at least 3 years of experience into networking and security and to have got entry level certificate	The course aims to provide an overview of cybersecurity risks in maritime domain, introducing the **Cyber-MAR concept** and platform (familiarisation)
Advanced	Users with high IT security skills, at theoretical and practical level. High security specialists may work as senior positions in IT departments. **Theoretical and hands on**	Mid-level certification plus direct experience on specific security environment , nice to have certifications on cybersecurity and vertical skills like CEH, Comptia Security +, CCDA and ISACA CISM and/or CRISC, but nice to have, not a must have	To provide a more detailed overview of cybersecurity risks and how good risk assessment will have a positive impact in reducing threats and vulnerabilities in the maritime sector also through the Cyber-MAR approach. The course will be updated with the latest tools on the use of the Cyber-MAR CR together with the recent international legislation and guidelines. Deep dive in cyberMAR and CR platform

WORLD MARITIME UNIVERSITY

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

Cyber-MAR training platform

Figure 1



Source: own elaboration

A/R/E	Academia, Research, Education
MT	Maritime technician
MO/ MM	Maritime Officer, Maritime management
ITT	IT Technical
O	Other
S	Seafarer

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

WORLD MARITIME UNIVERSITY

RESULTS

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.

.

WORLD MARITIME UNIVERSITY

RESULTS

The proposed platform in the present paper is under development.

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.

The platform will be its interoperability of different cyber-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.

RESULTS

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 a specific research could be dedicated to the the interoperability of the Cyber-MAR platform in the world maritime industries.

IMPLICATIONS FOR RESEARCH

Identification of the main gaps in maritime cyber security coupled with the training and awareness needs on cyber security aspects.

As mentioned in various reports on cyber preparedness “There’s no substitute for preparedness”.

Preparedness measures act as the umbrella that covers end to end the system and is fully operating even during the incident time. In effect, the preparedness level does not differ even when an incident happens.

THANK YOU FOR YOUR ATTENTION!