Cyber-security training platform on realistic maritime logistics scenarios

Presenter: Prof.
Dimitrios Dalaklis

WORLD MARITIME UNIVERSITY

Introduction:

- In the contemporary era, the issues of connectivity and interconnection are clearly standing out.
- The creation of the World-Wide-Web (Internet) and the integration of a literally unlimited number of information technology (IT) systems and people into a common collaborative environment has also created a very suitable tool to launch a variety od the so-called “cyber-attacks”…
- These malicious activities at a minimum could disrupt normal business activities (maybe even contribute into the creation of chaos, completely destabilising operations).

Introduction:

No matter the current "temporary difficulties" of COVID 19, the maritime sector still remains one of the most important sectors for today's global economy. Acting as the backbone of world trade, approximately 80-90% of goods and raw materials are "served" by the international shipping industry .

It is also true that 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 related maritime information systems.

Maritime information systems, whether on board of ships or in ports, are numerous, are built with standard components available on the market and in many cases designed without accounting for the cyber risk, which is ever growing.

Introduction:

Two two most known cases of cyber-attacks with devastating financial and societal impacts in this domain are:

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.

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 numerous 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 NotPetya malware:

- “How” did all these happened?

ASCII art of a skull and crossbones is displayed as part of the payload on the original version of **Petya**.

Ukraine has suffered for years as a cyberwar testbed…
Notpetya original version was designed to attack Ukrainian systems (it targeted systems with a common piece of Ukrainian bookkeeping software). To cut a long way short, it got out into the wild and shut down some of the world's largest companies, including Maersk, the world's largest shipper.
Avoiding extensive details, it did “significant” damage…

In Summary:

- The Maersk story shows how a system that fails in key ways becomes unusable, even if certain parts of it are unaffected: Maersk's shipboard systems were fine, but there was no way to distribute their loads or take on new cargo -- even the gates at the ports were frozen shut.
- After a frantic search that entailed calling hundreds of IT admins in data centres around the world, Maersk’s desperate administrators finally found one lone surviving domain controller in a remote office—in Ghana (Data there was not corrupted, because of a sudden power shutdown; pure luck…).

In Summary:

- At some point before NotPetya struck, a blackout had knocked the Ghanaian machine offline, and the computer remained disconnected from the network.

- It thus contained the singular known copy of the company's domain controller data left untouched by the malware—all thanks to a power outage.

- Established "Policies" and "Skilful IT Administration" failed to prevent the attack and its consequences!!!

“Where” exactly do we “stand” today?

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.

Shipping in the “Era of Digitalization”?

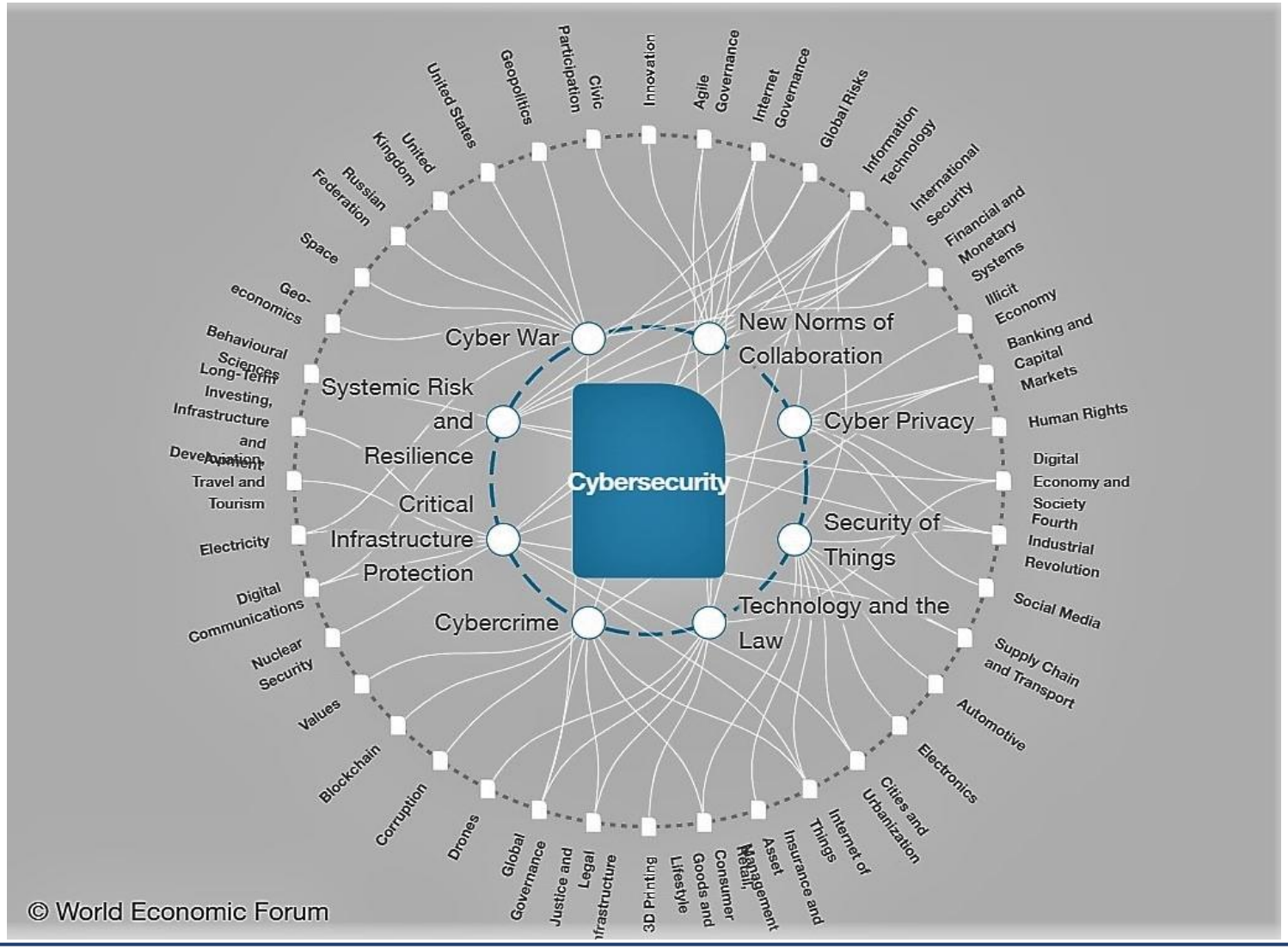
Objectives:

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.

Cybersecurity: Multiple “Connections”!



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”.

Data/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.

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.

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 organizations' 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.

Summary & Conclusion

- Recent discussions on the so-called “digitalization” phenomenon provide a very disruptive picture of how the shipping industry may be transformed in the near future.

- We should be concerned for the cyber-security threat, since there is already a heavy reliance on electronics, IT applications and software.

- The complexity of the cyber-security issue highlights a need to formalise/improve training requirements to ensure the secure & efficient conduct of operations.

World Maritime University

A Specialized UN Institution in Sweden

THANK YOU FOR YOUR ATTENTION!

IMO INTERNATIONAL MARITIME ORGANIZATION

WMU WORLD MARITIME UNIVERSITY