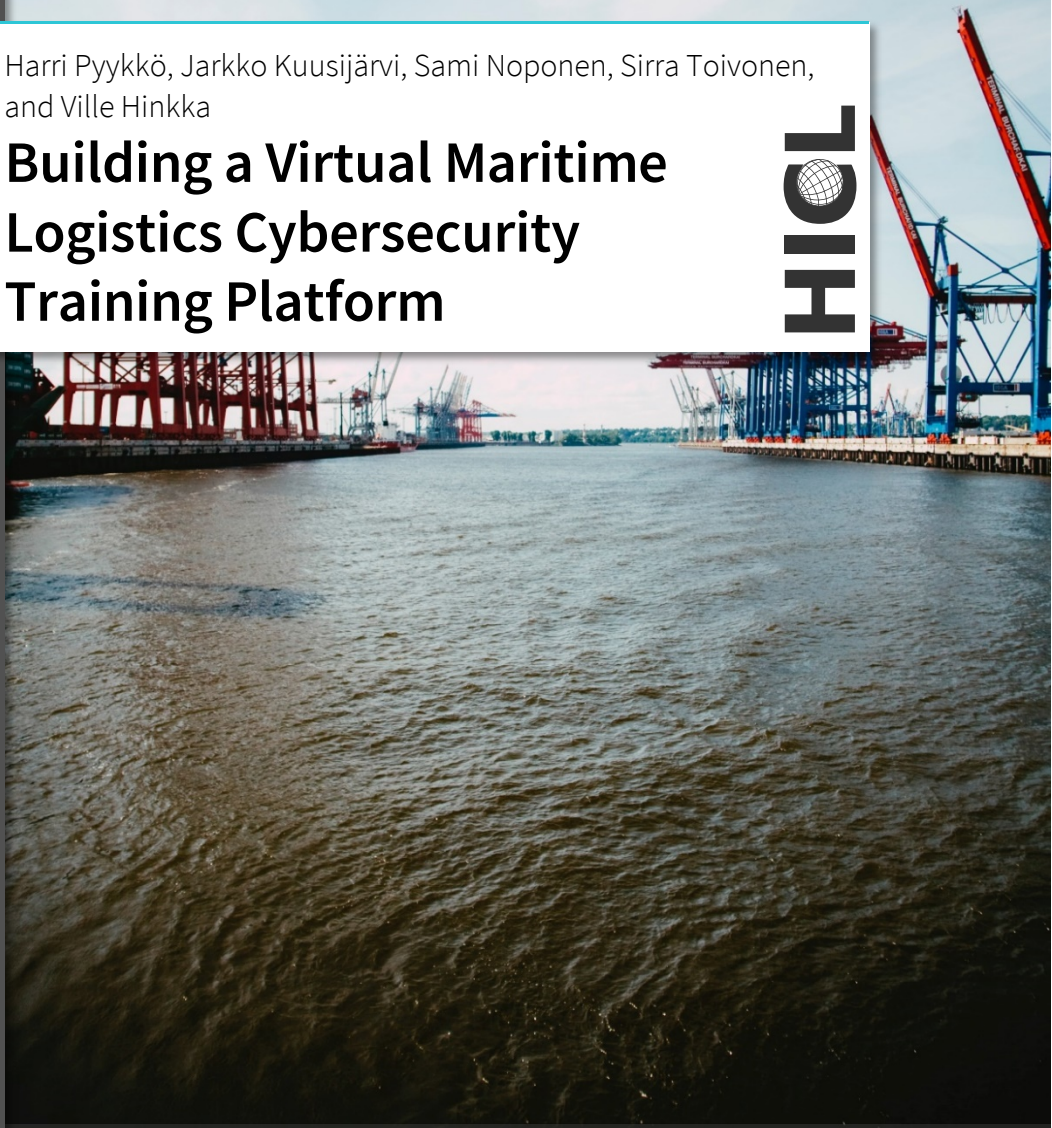
Harri Pyykkö, Jarkko Kuusijärvi, Sami Noponen, Sirra Toivonen, and Ville Hinkka

Building a Virtual Maritime Logistics Cybersecurity Training Platform

HICL



Published in: Data science and innovation in supply chain management
Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.)
ISBN: 978-3-753123-46-2 , September 2020, epubli

Building a Virtual Maritime Logistics Cybersecurity Training Platform

Harri Pyykkö [1], Jarkko Kuusijärvi [1], Sami Noponen [1], Sirra Toivonen [1], and Ville Hinkka [1]

1 – VTT Technical Research Center of Finland Ltd.

Purpose: This paper proposes how cyber ranges, which are simulation environments and platforms, can be used for cybersecurity training to reduce the vulnerability surface of the maritime supply chain caused by cyberthreat challenges. An additional benefit to conducting exercises for personnel with realistic environments is that unseen problems can be detected when training with different scenarios.

Methodology: This study aims to create a holistic model for a cyber range training environment customized for the port/maritime logistics sector by simulating the actual operational environment. The research combines cybersecurity and risk management with the special requirements of maritime logistics. The methods used were a literature review and a workshop and interview setup with cybersecurity, risk management and maritime professionals.

Findings: The demand for high-level resilience in global maritime supply chains, in addition to better business continuity management, is becoming increasingly important as global markets seek rapid responses to change. There are various new emerging technologies in the pipeline, which are rapidly gaining popularity in the logistics and supply chain management context. Cybersecurity preparedness is therefore essential.

Originality: Organizational and individual cybersecurity preparedness can be improved when individuals have access to hands-on training with realistic cyber exercise scenarios that cover different levels of interactions and triggers/injects in the actual environment. The training scheme focuses on training both technical and non-technical staff to provide extensive coverage of cyber awareness.

First received: 20. Mar 2020 Revised: 25. Jun 2020 Accepted: 8. Jul 2020

1 Introduction

The maritime sector relies heavily on complex Information and Communication Technology (ICT) and Industrial Control Systems (ICS). There are various new emerging technologies in the pipeline which are rapidly gaining popularity in the logistics and supply chain management context. This makes cybersecurity vitally important for the general operability of organizations and it should be deeply entrenched in organizational strategies. However, several recent studies (e.g., ENISA 2019, Ahokas & Laakso 2017) indicate that currently the maritime sector suffers from insufficient cyberthreat preparedness and poor awareness of general cybersecurity. Since ports are part of the critical infrastructure and maritime supply chains form the backbone of global trade, it is essential to increase cybersecurity and cyberthreat awareness and robustness against cyberattacks.

As technological development evolves at an accelerating rate, continuous training is essential for both professionals (cybersecurity experts, ICT experts, etc.) and non-technical personnel working within the maritime logistics cluster (Alcaide & Llave, 2020). This paper aims to determine how this training should be organized.

There are different options for organizing training. We focus on the possibilities of using cyber ranges (CRs), which are simulation environments and platforms for cybersecurity training, to reduce the maritime supply chain vulnerability surface caused by cyberthreat challenges. A further benefit of conducting exercises for personnel in realistic environments is that unseen problems can be discovered while training with different scenarios. This

can allow overall processes, technical functionalities and integrations between systems to be improved, increasing the overall efficiency of operations in normal conditions as well.

The starting point of this study is that cyber awareness will progress once individuals throughout the organization (not limited to IT-department or cybersecurity experts) can have actual hands-on training with realistic cyber exercise scenarios in the actual environment (Pyykkö et al. 2020). A CR can be used to conduct realistic cyber exercisers with industrial control systems reflecting typical features of maritime information technology/operations technology networks. It will also provide the counterparts to decision support in terms of cybersecurity procedure improvements and the need for further investments in corporate risk management tools. For training technical staff, detailed data such as alerts and logs are required with appropriate views. For training non-technical staff, a more holistic and easily understandable view, e.g. a dashboard, can be provided on the current cybersecurity situation. Both of these have to be included in the technical features of the CR.

This study aims to create a holistic model to build a CR training environment especially customized for the port/maritime logistics sector and simulating the actual operational environment. The research has a multidisciplinary approach, combining cybersecurity with the special requirements of maritime logistics. The methods used are a literature search and interviews with cybersecurity and maritime professionals.

2 Methodology

The methodology of this paper has two phases: 1) a literature search of cybersecurity threats in the maritime sector and 2) interviews with maritime logistics, risk management and cybersecurity professionals, including a workshop.

The main purpose of the literature search was to find out how the current academic literature considers cybersecurity threats in supply chain management and especially in maritime logistics. We were also interested in knowing what previous studies have found on how organizations view cyber risks compared to other risks.

The purpose of the interviews and workshop was to combine the expertise of different disciplines. The same people participated in both. The interviews were conducted before and after the workshop using an open discussion format in which interviewees could freely share their viewpoints. The workshop was a whole day event at VTT's cybersecurity lab, during which VTT's cybersecurity experts organized exercises demonstrating the vulnerabilities of existing information systems and how a CR could be used for training. The exercises were followed by discussions on the applicability of CRs for training in the maritime logistics sector. There were eight experts, three representing the maritime logistics sector, three cybersecurity, and two risk management.

3 Operational environment and particular features of maritime logistics

Maritime transportation is a vital link in global trade, and in the European Union area alone there are more than 1,200 active seaports. Each of these seaports has its own operational networks, organization, and physical and cyber infrastructure. (Enisa 2019) In addition to the fact that virtually all ports need customized solutions to fully meet their individual requirements, the rising level of digitalization is bringing new challenges for cybersecurity in both Information Technologies (IT) and Operation Technologies (OT) (Enisa 2019). ECSO (2020a) defines cyberspace as "the domain of information flow and communication between computer systems and networks and includes physical as well as purely virtual elements." In order to fully comprehend the cyberspace of the maritime logistics environment, a comprehensive overview is needed of the special features and complexities affecting this domain. Polatidis et al. (2018) underline that "Maritime port infrastructures rely on the use of information systems for collaboration, while a vital part of collaborating is to provide protection to these systems."

The holistic environment of maritime logistics contains multiple layers and various types of interconnections between numerous stakeholders. The literature review on maritime logistics networks (e.g. Dellios & Papanikas 2014) shows that generally, the maritime environment has two categories: the physical environment and the cybernetic environment, as shown in Table 1. The former includes stakeholders such as authorities, maritime, terminal and insurance companies, labour, and facilities including the port infrastructure. The cybernetic maritime environment contains the port infrastructure, ICT systems such as computer and telecommunications systems and networks, hardware, data, services and users (Dellios & Papanikas 2014; Polemi 2018).

Table 1: Division between physical and cybernetic maritime environments (Dellios & Papanikas 2014; Polemi 2018)

PHYSICAL ENVIRONMENT	CYBERNETIC ENVIRONMENT
Port infrastructure, facilities	Infrastructure, such as buildings and ships
Port authorities	Platforms such as servers and databases
Maritime and insurance companies	Telecommunication systems
Shipping and cargo industry	Software and manuals
Government ministries	E-services, such as applications
Related transport infrastructure	External users, such as maritime companies
Human resources	Internal users, such as personnel

In ports there are both IT and OT systems operating, but cybersecurity efforts have generally focused on the former, forgetting that physical operations controlled via OT systems need taking into account as well (Tam et. al. 2019). As described in Table 1, the overall operability of maritime supply chains and ports depends both on the physical environment and on existing infrastructures within the port areas, but also on continuous functionality of the cybernetic environment (Papastergiou et al. 2015).

The complexity of various IT/OT systems creates a system-of-systems that requires numerous types of interfaces connecting them together. According to ECSO (2020a), this is one of the key elements of cyberthreats in the

maritime industry. The ports are a vital part of maritime supply chains, and the information systems are closely linked to each other. Maritime end-to-end supply chain networks are highly complex, involving different types of international organizations that exchange information and data via their own information systems (Polatidis et. al. 2018).

3.1 Risk Management in maritime logistics

Ports play a major role as a global supply enabler, and they are often the key connection point for other transportation modes. The security of ports has been a key part of port management already for the last 20 years, since the global International Ships and Port Facilities Security (ISPS) Code became operational. Initially, the development focused on physical security, but in recent years cybersecurity and resilience management have gained increasing attention in response to a clear need arising from digitalization of port operations and processes and management of supply chains. However, digitalization poses major challenges to ports, as many of them still lack a digital culture in the port ecosystem. As a result, in many ports awareness regarding cybersecurity is still poor, and training, allocated budgets and resources lag behind what are considered real needs. Perhaps because of this, ports have been a prime target of cyberattacks in recent years, and stakeholders from many sides of the business have started taking serious steps toward managing cyberthreats. (Enisa, 2019) Chang et al. (2019) identified the following four major cyberthreats to the maritime industry: lack of training and experts, use of outdated IT systems, hacktivism, and fake websites and phishing emails. The International Maritime Organization (IMO) Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems (SMS) states that SMS should consider cyber

risk management, and encourages “Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021” (IMO, 2017). A holistic cybersecurity risk management, analysis and actions are therefore crucial for the maritime sector, ship operators and owners in the coming years.

The current demand-based market structure and lean supply chains have increased the supply chain complexity. The network is a target of many kinds of risk that have to be addressed efficiently. The investments made in security management have reduced supply chain disruptions. Conversely, the threat landscape has shifted towards cyberattacks and data breaches, and they have more often been mentioned as the main causes of disruptions (Elliot et al., 2019; Singh et al., 2019). As ports are major transportation network nodes, the cyberthreat is evident.

3.2 Supply chain resiliency and key performance indicators / KPIs

To succeed, a company’s supply chain should be resilient and its performance should be assessed accordingly. To guarantee timely action, cybersecurity should be clearly addressed in the ports' key performance indicators (KPIs). (Greenberg, 2018) Traditional supply chain resilience KPIs — which include measures for e.g. robustness, agility, visibility, IT capacity/information sharing, supply chain risk management (SCRM) culture, market position, risk control/revenue sharing, velocity and security — may address the cyber requirements for ports too generally. (Singh et al., 2019)

The frequency of port cyberattacks through e.g. malware, phishing, identity fraud, ransomware, man-in-the-middle attacks or data theft and their consequences is estimated to be greater than reported (Miranda Silgado, 2018). The current frameworks support identification, protection, detection, response and recovery in the risk management cycle to build operational resilience against cyberthreats. (International Maritime Organization, 2017). In addition to IT resources, the role of human resources and processes form important cybersecurity measures. (Mraković & Vojinović, 2019).

Because of the difficulty assessing return on investment (RoI) for security as well as for cybersecurity measures, there is no definitive consensus on KPIs. (Onwubiko & Onwubiko, 2019). At company level, the framework for cyber KPI metrics has been proposed to include the number of foiled (prevented, detected and intercepted) attacks, number of vulnerabilities and threats discovered, overage of business assets being monitored by the cyber management, human and process capabilities regarding managing, monitoring and reporting cyber incidents, monitoring capacity and capability of both technical and operational perspectives and incident detection capability. (Onwubiko & Onwubiko, 2019). Awareness and knowledge among port management, employees and the port network are key to timely control-measure actions. CR-enabled risk and security assessment enables ports to discover their weaknesses and vulnerabilities, assess mitigation measures, or evaluate, predict and practise the effectiveness of cyber risk management measures in general. (Polatidis et al., 2018)

4 Cyber range simulation set up

Cyber ranges are simulation environments and platforms for various purposes (ECSO, 2020b). They consist of multiple technologies that are used to construct an environment that has specific functionalities for end users. CRs are mostly used for security testing, security research and enhancing cyber capabilities and competence. A CR can be a general training platform for various aspects, or it can be a digital twin of a specific network environment. The size of a range varies; it can either be a cyber competition platform for up to thousands of users, or a training platform for a handful of participants. When the range is built for cybersecurity training purposes it is usually built or configured around a specific scenario and targeted set of users. Targeted users are usually pre-defined and the level of technical knowledge they possess has to be estimated in order to customize the training for them. Often the scenarios are targeted for ICT and cybersecurity professionals, but also for executive level or non-technical people who are essential when a real cyber incident takes place.

The basic building blocks of a CR are the same for any environment that is to be simulated inside the CR. The CR is composed of hardware (HW) and software (SW) components building up to the scenarios developed for a specific training scenario. Usually, the work required to create a new cyber exercise in a CR is focused on the specific new scenario and the related machines that need to be configured for it. Figure 1 shows how the workload is divided for specific parts related to a CR when constructing a new training (or even the first training); usually the customization and scenario building takes up most of the work for the CR/training organizers. Naturally, if the

new scenario is close to a previously built one, the workload drops significantly.

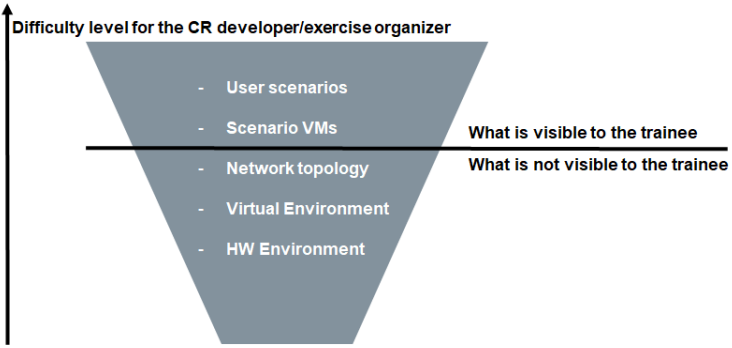


Figure 1: CR, what is visible to the participants, and the effort required to build the scenario.

VTT's CR has been built for organizing small cyber exercises on specific themes. It is hosted on a rack server, the network side is virtualized, and the computers used in the exercises are running in virtual machines. It enables the simulation of cyberattacks and defences, identification of threats and vulnerabilities, traffic monitoring and in-depth analysis. It consists mainly of customized workflows for setting up the scenarios with virtualized systems. Participants use a remote desktop or similar for connecting to the environment. Organizers can use remote or local connections to set up scenarios and control specific training sessions. Figure 2 shows the basic building blocks of a CR operated by VTT, emphasizing components that usually

need tailoring according to scenario-specific needs, such as monitoring, situational awareness and obviously the specific machines (virtual systems) for a given maritime scenario.

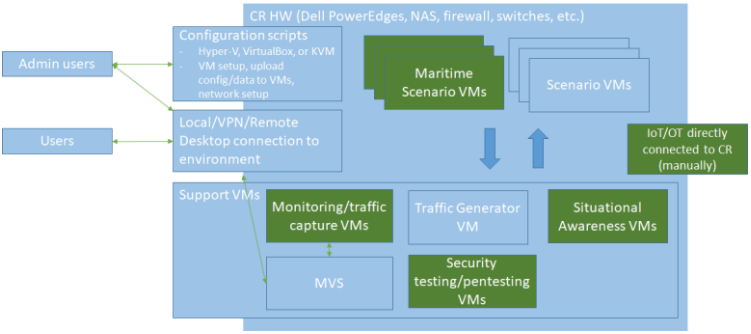


Figure 2: Building blocks of a CR for maritime cybersecurity training

4.1 How to adjust cyber range simulations for the maritime cyber domain

The knowledge of how to build the specific modules used in a scenario is heavily based on the user and operational requirements. Depending on the scenario, the IT/OT devices of the specific scenario, the CR will have to introduce various different network segments and machines located in these network segments. Usually, in a maritime specific scenario, the inclusion of OT devices is obvious. These OT devices can be included into the environment by adding real HW devices that are connected to the virtual environment, or they can be introduced by including virtual OT devices into the vir-

tual environment. The goal of the whole CR scenario work is that the environment (software systems and tools) used by the people in the CR environment is as close to the real environment as possible. This enables to educate and train the people according to the various cyber-related risks/attacks that may occur in their specific environment and how to react to them.

Additionally, we can use the CR environment to test out a new system(s) in a realistic setting without introducing it into the normal operational environment. In addition to covering normal user guidance and testing of functionalities, we can test the system for any cyber-related incidents that may be introduced by integrating it into the current operational environment. Combining two or more functional systems may not always result in one functional operational system, especially in terms of cybersecurity, as there may be some compromises that have to be made in order to integrate systems that might be noticed only during 'normal operations'. The whole purpose of using a CR is to train the operators of the system(s) in the abnormal situations occurring while using the systems. Thus, organizing a CR cybersecurity exercise/training introducing a new system may well introduce some technical and/or (cybersecurity) process-related issues that can then be solved before actually taking the system into everyday use.

The port logistics system running in the CR does not have to be replicated as an exact twin of the real system. It is usually enough that the simulated components provide meaningful functionality for the scenario. For example, a component can be simulated just by replaying relevant traffic into the CR network. Training scenarios often include a simulated cyberattack that can be executed by the organizers or participants playing as a red team. The attacks are often scripts that execute malicious files or inject traffic into the

system. Participants have to detect the attacks with the provided tools and react accordingly.

The following list of components provides examples of what can be virtualized in a CR for maritime/port logistics specific scenarios:

- Ship location tracking (GPS, AIS)
- Weather data and forecasts
- Electronic cargo and passenger manifest systems
- Cranes and other container handling systems
- Container tracking systems
- Human-machine interfaces
- Remote diagnostics and maintenance

Situational awareness of the exercise is an important topic for the participants to see what is happening in the environment. Situational awareness can be coarsely divided to two views, depending on the user's needs: high-level and low-level views. During the exercise it is possible to display data of different aspects for people with different competences. For example, technical cybersecurity professionals would be presented with e.g. detailed log data, Intrusion Detection System alerts and network data packets. Different data would be presented for the non-technical people, e.g. risk-analysis, operational status of SCADA systems, or textual descriptions.

4.2 Implementation of a cyber range-based training platform

Defining learning goals for the participants is an important part of planning the pedagogical side of the training. The learning goals are set out in the

planning phase, carried out in the implementation (exercise) phase, and finally recapped in the feedback phase after the exercise (Karjalainen et al., 2019). Karjalainen et al. (2019) also argue that specific technical phenomena may distract the users from achieving the actual learning goals that are being targeted for the users. Our approach to tackling this gap is to gather knowledge about the participants' background knowledge, weaknesses and strengths, in order to customize the training around the discovered learning goals. After the CR environment including all the required components and the training scenarios has been developed, preparations for organizing the training session can begin. As maritime logistics involves a large number of different stakeholders, especially at ports where all the different stakeholders come together and interface with each other, it is important to gradually train the stakeholders in their own environments first. After the personnel have been trained to successfully operate, protect and react to possible cyber incidents in their relevant operational environments, the stakeholders can also participate in a wider training/cyber exercise where especially communications skills and co-operation with the relevant other stakeholders can be trained. The following lists possible roadmap steps in realizing this overall training scheme, building up from gathering the existing knowledge, building the scenarios, and ending at a collaboration exercise between selected stakeholders that interface with each other. It should be noted that, depending on the learning objectives and skills of the participants, the CR can be utilized in one or all of the steps listed.

Step1: Online questionnaires/exercises. The purpose of this step is to ascertain the overall skill level of the people participating in the training. Simple exercises can also be done online in a Moodle or even in the CR.

Step 2: Online security awareness training. The purpose of this step is to train the people before jumping to the CR environment, in case they are new to cybersecurity and/or need/want to train themselves beforehand.
Step3: Specific CR exercises for separate groups. The purpose of this step is to organize specific training sessions for different personnel groups. These groups can range from non-technical people to cybersecurity professionals. The target is to train their cyber skills and combine their knowledge while they are working together on specific scenarios. This is targeted to one or more specific operational parts and cybersecurity aspects.
Step4: Intra-company-wide CR exercise/training. The purpose of this step is to have a more large-scale cyber training/exercise with most of the people from the organization taking part. The aim is to train and try out the company's cybersecurity policies during a cyber incident. It will also help to exercise communication between the key roles in the company in case of an incident; who will handle what, who to contact in case of incidents, etc.
Step5: Inter-company-wide CR exercise/training. This is an optional final step, in case e.g. the port authority can organize a larger exercise that includes people from multiple stakeholders. It should also have a scenario in which all of the stakeholders would operate their own systems as in reality and train how a cyber incident is communicated and how it is handled in co-operation between all the relevant stakeholders. This type of training can also include non-technical trainings, such as how to communicate the incident to the outside, like media (incident reporting to CERT/CSIRT is part of the technical part). Figure 3 shows in what relation the different proposed steps are located compared to the exercise/CR preparation work

(feedback is about the CR exercises, otherwise feedback should obviously be available after each step).

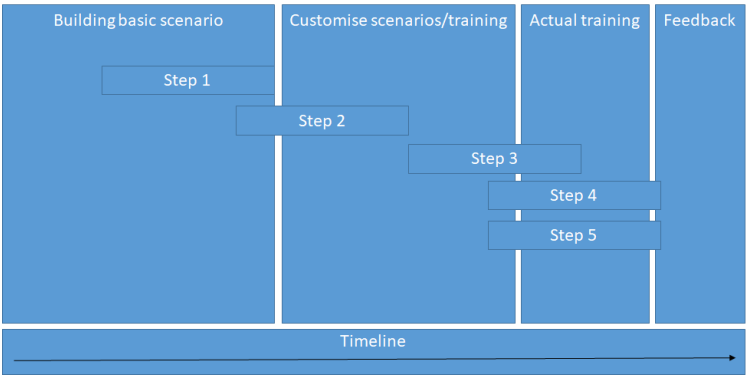


Figure 3: Training steps and CR development/usage phases.

5 Conclusions

As the general level of digitalization and automation of operations continues its rapid growth, also in maritime logistics, it is crucial for overall cybersecurity preparedness that maritime organizations guarantee their personnel appropriate and thorough training, ranging from IT specialists to basic end-users of the systems. As long as there are human factors affecting system usage, not even highly advanced cybersecurity technologies can alone bring sufficient cyber-protection coverage against cyberattacks.

The starting point of the study and related workshop was to combine cybersecurity research with the particular features of maritime logistics, in order to gain a holistic model which can then be utilized when designing the CR training platform. A multidisciplinary approach is needed to close the knowledge and communication gaps between cybersecurity and maritime logistics research and create a mutual learning process. Increasing implementations of new emerging technologies to existing maritime processes will also increase the need for comprehensive cybersecurity simulations and tailored training before the new implementations can be taken into operational use.

The complexity of the maritime logistics environment and general lack of cybersecurity standards is generating pressure for individual maritime organizations and ports to guarantee that cybersecurity preparedness and technological competencies of their own systems, interfaces and personnel are continuously up to date in order to decrease the cyber risks. When creating the CR training scenarios, it is also important to recognize the diversity of different contextual settings and participants' individual skills.

Developing the baseline and the first training scenarios in the CR are the most time-consuming tasks when creating a training for a new context, such as maritime logistics/ports. Once the target core systems and first detailed scenarios are developed, adding new scenarios based on the existing systems and/or introducing a similar system to the CR is a much lighter task. The scenarios and related situational awareness implementations can be reused extensively when moving the training into a new similar environment, e.g., a new port with a different set of systems in use. Obviously, any new system has be to implemented/replicated into the CR if it is crucial for achieving the training goals, but the overall scenarios mostly stay the same. Once the maritime organizations have a validated risk management set up, it should possible to recognize the weakest points of systems/operations. This is valuable information to be given to the training organizers/operators of the CR. The requirements management process in the organizations has to consider these cybersecurity-related requirements/risks as well and how these could be mitigated. The EU Directive on security of network and information systems/NIS (pl, art.3) highlights that cybersecurity should not be considered purely as a technological but also as a strategic issue that the organizations themselves are accountable for (NIS 2016).

6 Discussion

The European Cyber Security Organization (ECSO, 2020a) estimates that globally only around half of existing ports have a sufficient level of understanding in terms of their own cybersecurity aspects, which translates into an urgent need for improvement. The demand for a high level of resilience in global maritime supply chains is an increasingly important aspect of this, alongside business continuity management as global markets consistently require fast responses to change. The common trend is for cargo flows to be as seamless as possible to avoid warehousing of goods. In general, this means that manufacturing companies will have very limited buffer stocks in case of disruptions in the supply chain, while at the same time being ever more dependent on ICT systems. These advances create pressure for manufacturing companies, logistics service providers and ICT companies worldwide to put additional effort into their supply chain operability taking into account potential disturbances in normal material flows.

Training designed for the most technically skilled cybersecurity professionals is certainly not something to challenge normal users of the systems with. Pedagogically, the training must be tailored to the student — start with the basics, then move towards the more complicated learning goals that require prior knowledge. One hurdle to cross in cybersecurity (hands-on) trainings/exercises is that not everyone attending may be right for the level of difficulty of that specific exercise. Some may be highly skilled at cybersecurity while others are at the start of their learning curve. If the exercise is not effective for most of those participating in it, it helps neither the participants nor those running it. Therefore, we emphasize the importance of selecting appropriate participants for specific exercises and trainings.

The most suitable solution would be to conduct a pre-exercise quiz or small-scale online exercise to assess skill levels, allowing the organizers to focus the exercise on the specific weaknesses of the participants. Better yet, they could suggest that the organization willing to educate their personnel divide the participants into one or multiple groups based on training needs. This decision is, of course, up to the organization joining the exercise.

Acknowledgment

This work has received funding from The European Union's Horizon 2020 research and innovation program under grant agreement No. 833389.

References

Ahokas, I., Laakso, K., 2017. Delphi study on safety and security in the Baltic Sea Region ports. Publications of the HAZARD Project. Available at: <https://blogit.utu.fi/hazard> Accessed 30 April 2020].

Alcaide, J.I. and Llave, R.G., 2020. Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, pp. 547-554.

Chang, C.H., Wenming, S., Wei, Z., Changki, P. and Kontovas, C.A., 2019. Evaluating cybersecurity risks in the maritime industry: a literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference.

Dellios, K, Papanikas, D., 2014. Deploying a Maritime Cloud. IT Professional, 16(5), pp. 56-61.

ECSO 2020a. ECS WG5 PAPER Understanding Cyber Ranges: From Hype to Reality. Available at: <https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf> [Accessed 12 May 2020].

ECSO 2020b, Transportation Sector Report 03/2020, Cybersecurity for road, rail, air and sea, WG3 / Sectoral Demand. Available at: <https://ecs-org.eu/documents/publications/5e78cb9869953.pdf> [Accessed 12 May 2020].

Elliot R., Muhammad, K., Reece, D., 2019. Supply Chain Resilience. 10 Year Trend Analysis. BCI. Available at: <https://www.thebci.org/uploads/assets/uploaded/6bd728bd-bf0e-4eb7-b15fa67164eb9484.pdf> [Accessed 22 May 2020].

ENISA (2019), Port Cybersecurity - The good practises for cybersecurity in the maritime sector, October 2019

Greenberg A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired August 22, 2018. Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> [Accessed 10 May 2020].

International Maritime Organization, 2017. Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3. Available at: <http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf> [Accessed 10 May 2020].

IMO, 2017. Resolution MSC.428(98), Maritime Cyber Risk Management In Safety Management Systems, 2017. Available at: < http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf> [Accessed 10 May 2020].

Karjalainen, M., Kokkonen T. and S. Puuska, S., 2019. Pedagogical Aspects of Cyber Security Exercises. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Stockholm, Sweden, pp. 103-108,

Miranda Silgado, D., 2018. Cyber-attacks: a digital threat reality affecting the maritime industry. World Maritime University Dissertations. 663.

Mraković, I. and Vojinović, R., 2019. Maritime Cyber Security Analysis–How to Reduce Threats?. Transactions on maritime science, 8(1), pp. 132-139.

NIS (2016), The Directive on security of network and information systems, p1, art. 3., Directive (EU) 2016/1148 of the European Parliament and of the Council.

Onwubiko, C. and Onwubiko, A., 2019. Cyber KPI for Return on Security Investment. In International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, United Kingdom, 2019, pp. 1-8.

Papastergiou, S., Polemi, N. and Papagiannopoulos, I., 2015. Business and threat analysis of ports' supply chain services. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 642-653). Springer, Cham.

Polatidis, N., Pavlidis, M., Mouratidis, H., 2018. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Computer Standards & Interfaces, 56, pp. 74-82.

Polemi, N., 2018. Port Cybersecurity - Securing Critical Information Infrastructures and Supply Chains. Elsevier

Pyykkö, H., Kuusijärvi, J., Silverajan, B., Hinkka, V., 2020, The Cyber Threat Preparedness in the Maritime Logistics Industry, Research Arena 2020, Helsinki, Finland, 27-30 April, 2020. (Conference cancelled)

Singh, C.S., Soni, G. and Badhotiya, G.K., 2019. Performance indicators for supply chain resilience: review and conceptual framework. Journal of Industrial Engineering International, Vol. 15, pp. 105–117.

Tam, K., Jones, K., Forshaw, K., 2019. Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities. International Conference on Marine Engineering and Technology (ICMET), Oman.