

World Maritime University

# The Maritime Commons: Digital Repository of the World Maritime University

---

Articles

Library

---

2021

## CR CyberMar as a Solution Path towards Cybersecurity Soundness in Maritime Logistics Domain

Monica Canepa

Fabio Ballini

Dimitrios Dalaklis

Seyedvahid Vakili

Luis Miguel Colmenares Hernandez

Follow this and additional works at: [https://commons.wmu.se/lib\\_articles](https://commons.wmu.se/lib_articles)

---

This Article Open Access is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact [library@wmu.se](mailto:library@wmu.se).

# CR CyberMar as a Solution Path towards Cybersecurity Soundness in Maritime Logistics Domain

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

Cybersecurity is now considered as one of the main challenges for the maritime sector. At the same time, the maritime transport industry remains one of the most relevant and driving sectors for the global economy in terms of both the number and operations of active companies, and infrastructure and investments, thanks to the policies pushed to attract the latter. Maritime information systems, whether on board ships or in ports, are numerous, built with standard components available on the market and in many cases designed without factoring in well the ever-growing cyber risk.

Digital infrastructure has become essential in operating and managing systems critical to the safety and security of shipping and ports. Specifically, Cyber-MAR is focused upon the simulation and emulation of the real world of maritime systems (e.g. Logistics, Supply Chain). This research effort will examine the creation of a federated Cyber Range (CR Cyber-MAR) which will include various platforms and interconnected systems on board

## KEY WORDS

- ~ Maritime cyber security
- ~ Training needs
- ~ CYBER-MAR project
- ~ Cyber range

World Maritime University, Malmö, Sweden

e-mail: [moc@wmu.se](mailto:moc@wmu.se)

doi: 10.7225/toms.v10.n01.011

This work is licensed under 

Received on: Nov 26, 2020 / Revised on: Jan 4, 2021 / Accepted on: Feb 11, 2021 / Published: Apr 20, 2021

a vessel or ashore, in order to allow a hyper-realistic simulation of cyber-attacks and trying to assimilate them into real-life. Then the identified CR Cyber range will be integrated in the Cybersecurity training needs for different levels of operators.

The investigation of the discussed topic will essentially use qualitative techniques, analysing data obtained from publications, official and commercial reports, and interviews of a targeted audience.

## 1. 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 computer systems and people into a common collaborative environment has created the opportunity to launch various types of cyber-attacks that, at a minimum, could disrupt normal business activities (Dalaklis and Schröder-Hinrichs, 2019). In recent years, the use of digital means has been rapidly expanding throughout the whole world, the maritime industry being no exception; shipping companies are relying on a very extended number of computers and information technology (IT) applications to effectively support their business activities. At the same time, the safe conduct of navigation is heavily supported by a significant number of interconnected electronic systems and various digital means (Dalaklis et al., 2020). Effectively dealing with the issue of “Cybersecurity” should be a high priority issue, especially when factoring in the fact that the world’s economy is continuing its transformation towards a digital paradigm. As a result, professionals with a very dedicated focus will be needed to cover whatever gap is created

by the advance of the so-called “digitalisation phenomenon” and the associated cyber risks. This in turn is indicating a need for continuous training activities to add more resources in the workforce pool, who should be equipped with the “right” skills and fully updated with the newest IT trends.

Despite the difficulties created by 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 nowadays by the international shipping industry. It is also useful to note that the numerous information systems supporting the different functions of the maritime transport industry - whether on board ships or in ports - are built with standard components available on the market and in many cases designed without factoring in well the cyber risk, which is ever growing. The lack of awareness about cyber threats is evident in several different business sectors, including the maritime one (Canepa et al., 2020). In this paper, the needs and challenges relating to cybersecurity training will be analysed. In order to investigate possible solutions, the cyber-MAR project will be presented first, as it will use a federated Cyber Range solution being part of a cybersecurity training platform dedicated to the maritime sector peculiarities. The methodology implemented is based on a qualitative approach: a literature review and an analysis of the target groups will be involved in the Cyber-MAR training develops under the Cyber-MAR project (IT preparation actions for a holistic approach and awareness raising in the supply chain of maritime logistics). This project (funded Horizon 2020 Programme), lasting three years, started in September 2019, aiming at to achieving the following objectives: “to fully unlock the value of using the cyber range in the maritime logistics value chain through the development of an innovative simulation environment that adapts to the peculiarities of the maritime sector and is at the same time easily applicable to other transport sub-sectors”.

In addition, it aims at covering the training needs of all professionals (cyber / IT security experts, non-IT personnel of ports, shipping operators, related entities affected by possible cascading effects), as well as increasing the level of awareness of cyber threats within these organisations through hand-on exercises.

The Cyber-MAR platform about to be developed is under discussion, whereas the related intermediate advanced training offerings are still under development, with some more “fine-tuning” being required. The main expected results are the following: a) Ensuring that cybersecurity and IT professionals can easily create actual or fictitious cyber-attack scenarios in a simple way; b) Raising the level of qualification of professionals and experts who will be able to count on a training carried out on a platform that will guarantee high interoperability of different cyber-range systems.

## 2. CYBERSECURITY SKILL SHORTAGE

Recent discussions on the “digitalisation phenomenon” and maritime autonomous surface ships (MASS) provide a disruptive picture of how the shipping industry may be transformed in the near future (Kitada et al., 2018). The industry should be concerned with the cyber-security threat, since there is already a heavy reliance upon electronics and software/IT applications. According to (De Zan and Di Franco, 2019), the demand for cybersecurity job positions has increased its rate in the IT vacancies as a whole. Furthermore, the salaries associated with the cybersecurity domain have a 16 % premium over other the IT related ones. An effective covering of these (cybersecurity) positions took 20 % longer time than other IT vacancies during the year 2013. This cybersecurity skill shortage has been observed during last years, even during 2020. In this regard, (Security, 2020) is pointing out that “*Cybersecurity demand is twice as great as supply*”, indicating the need to retrain employees working in different sectors inside their companies in order to satisfy the need for staff with the “right skills”.

Similarly, ((ISC)<sup>2</sup>, 2019) estimates the workforce of specialists on cybersecurity to be around 2.8 million - by using the data based on eleven specific economies – also estimating a global gap to be close to 4.07 million, therefore creating an urgent need to expand the available human resources by 145%. At the same time, even by using data for a very particular economy (Saleh et al., 2020) described a scenario where only in the US “*for every 100 job postings (related to Cybersecurity), we estimate there are only around 48 qualified candidates*”. This clearly implies an obvious necessity for more professionals, and even though these numbers are related to just one country, they are also reflecting a global trend. Finally, in the EU, several member States have already pointed out that cybersecurity skills shortage is a real problem and the need for education/training in this matter is affecting not only the economy, but also their public sector (De Zan and Di Franco, 2019).

## 3. CHALLENGES IN CYBERSECURITY EDUCATION AND TRAINING

Cybersecurity is considered to be an extremely specialised domain. There is a very fast pace of change associated with it and the present curricula for education and training at universities need to be revised on an on-going basis. Quite often there are gaps between real requirements and academic offerings, considering that technology evolves at a high speed. In this regard, graduates from Universities may often receive a formal education that is not aligned with the current topics, not being quite prepared to face the needs of their employer right away; a skill mismatch is therefore identified (De Zan and Di Franco,

2019). It is indicative that Gagliardi et al. (as cited in De Zan and Di Franco, 2019) describe a need for teaching computing and cybersecurity issues even before joining a university, as an integral part of formal education. From the previous statements, it becomes clear that first, cybersecurity training offerings must be continuous and dynamic, and second, it must be considered as a matter of public, private, social, and educational interest. In addition, cybersecurity issues related education and training activities should take into account simultaneously technical, social, and legal aspects in order to provide an adequate response to the market's demands.

Furthermore, a significant challenge faced by education and training activities, with a focus on cybersecurity, is the difference in how they are conducted from one country to another. For instance, Vishik and Heisel (as quoted in De Zan and Di Franco, 2019) commented that even in the EU, where policies follow common objectives, it is a challenge to keep similar approaches to education in these matters. Also, they explained that there is a *"lack of cybersecurity educators, poor interaction with the industry, little understanding of the labour market, outdated or unrealistic platforms in education environments, and difficulties in keeping pace with the outside world"*. Finally, after highlighting all the previous challenges, it seems self-explanatory that the wider framework of "formal" education and training for cybersecurity should require adjustments and improvements. However, due to the complicated relationship between students, graduates, academia, and the outside world, the stakeholders involved have not yet reached consensus on cybersecurity training that would effectively respond to the real market's needs.

#### 4. CYBERSECURITY EDUCATION: EVOLUTION OF THE DISCIPLINE

Cybersecurity has come to be considered as a need, even before the implementation of what is nowadays known as the Internet. To put an indicative point of time forward, it began in 1971 with the attempt to test the mobility of programs through a network during ARPANET times (SentinelOne, 2019). Although the intention was not to create a disruption, the program under discussion replicated unexpectedly, causing an abnormal behavior of the whole system. From this starting point, people involved in computer science and the digital world have realised the importance of protecting information from external intruders. Nevertheless, another key point in time was 2011, when the National Initiative for Cybersecurity Education (NICE) began to define the NICE Cybersecurity Workforce Framework as a common language for cybersecurity work and the required tasks and skills (Cabaj et al., 2017).

Then in 2013 the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) included in their curricula guidelines relating to

Information Assurance and Security Knowledge Area (IAS KA). These institutions were putting emphasis on *"the Core Leadership Group... felt that it was premature to produce curriculum guidelines beyond CS2013, as they considered that cybersecurity was an immature and ill-defined subject"* (Cabaj et al., 2017). Furthermore, agencies like the National Security Agency (NSA) and Homeland Security in the US, promoted programs like the National Center of Academic Excellence in Cyber Defense two or four year program dealing with Information Assurance (IA), Cyber Defense, and "Policy, Legal, Ethics, and Compliance". In 2017, the Joint Task Force of "ACM-IEEE-Association for Information Systems Special Interest Group on Security" published the Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity with six main topics: Data Security, Software Security, System Security, Human Security, Organisational Security and Societal Security.

#### 5. AN INTERDISCIPLINARY /MULTIDISCIPLINARY APPROACH FOR CYBERSECURITY EDUCATION

Due to nature, objectives, and business areas where cybersecurity is applied, it is quite imperative that professionals involved in the specific domain have a background spanning into various different disciplines. The rationale behind this argument comes from the intrinsic need for understanding the different levels of operation so *"the members of the cybersecurity team will examine each business process to determine acceptable levels of risk"* (Blair, Hall, and Sobiesk, 2019). Viewed in a perspective, these teams will eventually include a mix of human experts and (support by) Artificial Intelligence (AI); the idea is to integrate professionals from computing science and targeted areas to *"identify, utilise, and develop innovations that facilitate stability and operational success across the organisation, society, or nation state"* (Blair et al., 2019). These teams size should vary, depending on the "targeted mission", and must be adapted to a particular need or activity.

Moreover, integrating professionals with different areas of expertise (computing science, statistics, systems engineering, economics, mathematics), try to make it feasible to provide a product (software, networking defences, etc.) effectively complying with all relating laws, policies, and regulations. At the same time, different perspectives must be considered while creating protocols and processes to protect information, networks, and software, such as criminology and relevant forensic procedures, thereby understanding rationality, crime scripts (attack trajectories), and finally pushing forward best practices in order to facilitate crime prevention (Rege, 2015). In addition, there is a need to consider input from disciplines like Psychology (considering the human element interacting with the systems from the defenders' and attackers' perspective); Law; Political Science and International Relations in order to understand the regulatory framework related to cybersecurity; Business and

Management to understand acceptable levels of risk and nature of the business in the organisation (Blair et al., 2019).

## 6. THE IMPACT OF CYBERSECURITY AWARENESS

Awareness is crucial, regardless of the field under consideration: this is especially true of Cybersecurity. It is also necessary to highlight that Cybersecurity deals with information security at the personal level, often involving issues at the organisational one. Activities such as browsing and disclosing personal information, installing software, and sharing information with third parties, can have various “*spill over*” effects at any organisation. Quoting the Information Security Forum, (Alruwaili, 2019) comments that “*security awareness is a continual process of learning by which trainees realize the importance of information security issues, the security level required by the organisation, and individuals’ security duties*”. Hence, this process is relevant and inescapable to provide a proper understanding, planning, and improvement of cybersecurity procedures. Nevertheless, due to the nature of cybersecurity’s stakeholders, the wider process of awareness and training must be interesting, capturing the attention of the targeted audience and easy to be followed by them, regardless of the level of knowledge in computing science. Furthermore, an emphasis on the psychological aspects relating to risk assessment and behaviour analysis should also be integrated in the whole process. In summary, the importance of cybersecurity awareness is based on the fact that the lack of it increases the risks of attacks and opens up numerous undesirable vulnerabilities in the IT systems supporting any company and organisation. Or, as emphasised in numerous reports and research efforts with a similar scope: “There’s no substitute for preparedness”.

## 7. THE EU DIGITAL AND CYBERSECURITY EDUCATION POLICY

Regarding the wider Digital and Cybersecurity Education Policy currently in place, in 2013 the European Union (EU) developed the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. This policy aims at creating and improving education and training related to network and information security skills and competence of IT professionals as well. Additionally, the EU has recently realised that it was 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 the same way, in 2017, via “Resilience, deterrence and defence: Building strong cybersecurity for the EU”, it was recommended to Member States to enhance cybersecurity education and skills; build digital skills and jobs, apprenticeships; launch e-government

and awareness campaigns; establish industrial, technology and research competence centre(s) and a network of national and European cybersecurity. In 2019 four projects linked to European cybersecurity competence network, research and innovation roadmap were launched within the Digital Education Action Plan frame. Finally, in the respective Digital Education Action Plan (2018 - 2020), Priority 2: Developing digital competences and skills, Action 8 - Training in digital and entrepreneurial skills for girls, the EU promotes a policy of gender equality regarding access to studies and careers aiming to increase the participation of women in the Information and Communication Technologies (ICT) and Science, Technology, Engineering and Mathematics (STEM) fields, breaking the stereotype of a male dominated industry (European Commission, 2018).

## 8. CYBER-MAR TRAINING PLATFORM

Within the Cyber-MAR project under discussion, a combination of innovative technologies aims at creating the Cyber-MAR platform which will focus on hyper-realistic simulation and emulation of maritime systems (e.g. Supply Chain), also aimed at creating a Cyber federation Range (CR Cyber-MAR), which will include various platforms and interconnected systems aboard a ship or on land, in order to facilitate a real-time simulation of cyber attacks and potential harmful consequences.

The Cyber-MAR platform offers a unified framework with intrinsic bidirectional interfaces between Cyber-MAR CR, the MaCRA framework for risk analysis and assessment and econometric models.

By developing the risk assessment framework to quantify the impact of cyberattacks in the maritime sector, a series of relevant econometric models will be created that will assess the potential economic impact across different value chains due to various cyber attack scenarios. The CyberMAR econometric model will be able to offer decision support to companies and government organisations in identifying and assessing their potential risk to promote mitigation strategies accordingly. Furthermore, the resulting outcomes relating to potential economic losses would offer users the possibility of the sustainability of planned investments in cyber defense products, so that they can estimate the potential benefits of such purchase and change in their IT infrastructure. Table 1 below, describes the training levels identified for the Cyber-MAR training and target groups that have been identified to attend the training course. To get a better understanding of the cyber-attack portfolio that can be used within the maritime domain and maximise the associated learning outcomes, the targeted audience was divided in three different categories, based on their familiarisation with the topic:

**Entry level:** will consider the theoretical aspects of the issue to make the audience more familiar with cyber security.

Table 1.

Description of the training levels and target groups identified.

Complexity level	Details	Requirements	General aims
<b>Entry level</b>	Entry-level users who are not familiar with cyber security <b>Theoretical</b>	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.
<b>Mid-level</b>	Users who are familiar with cyber security and wish to increase their skills to a higher level <b>Theoretical and hands on</b>	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 <b>Cyber-MAR concept</b> and platform (familiarisation)
<b>Advanced</b>	Users with high IT security skills, at theoretical and practical level. High security specialists may work as senior positions in IT departments. <b>Theoretical and hands on</b>	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	The course aims 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

The Cyber-MAR course will cover the basic introduction to cyber security according to the concept of the Cyber-MAR. This will lead to raise awareness among identified users (a very large audience) and provide the participant with the opportunity to understand cyber security threats and the basic concepts for reducing risk in the maritime sector.

**Mid-level:** Will make the users more familiar with the topic, especially those that are enthusiastic to promote their knowledge and skills and bring it to a higher level. The course aims to provide an overview of cybersecurity risks in the maritime domain, as well as to introduce the Cyber-MAR concept and its related platform.

**Advanced level:** Will be useful for Users who are already equipped with high IT security skills, as well as practical experience. These specialists may work in senior positions in IT

departments. The course in this level will provide a more detailed overview of cybersecurity risks, as well as help to determine what the effective risk assessments will be in reducing threats and vulnerabilities in the maritime sector by fully exploiting the Cyber-MAR approach.

The LMS - Entry-level call for training has got applications from different target groups, as shown in the Figure 1.

The number of applications received has been 123, composed as follows: the "maritime officer" and "maritime management" represents almost half of applications, followed from "academia, research and education" group. The "Others" (10%), includes consultants and journalists. Approximately 6-7% of "IT technical", "seafarer" and "maritime technician" applied.

## Entry level applicants by target groups

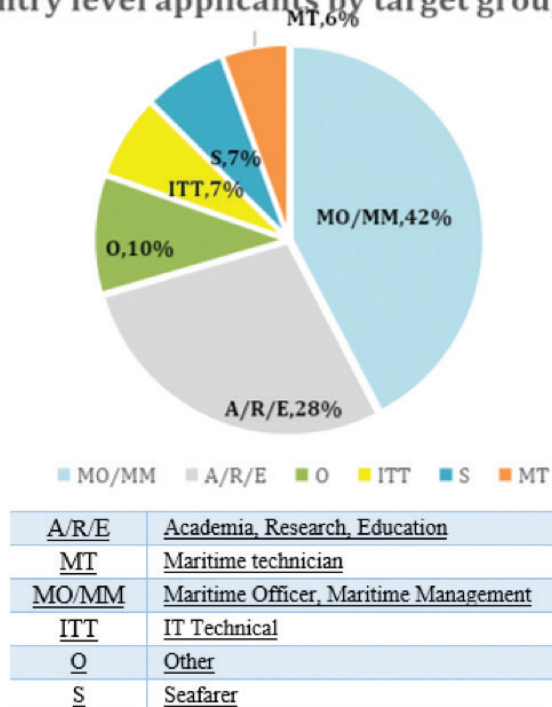


Figure 1.  
Entry level applicants by target group.

## 9. CONCLUSION

History testifies that there is a dialectic relationship between humans and technology. A report under the title "Transport 2040: Automation, Technology, Employment - The Future of Work", which has recently been launched by the World Maritime University (WMU), is rightly emphasising that: "Technological progress and innovation have occurred throughout history and changed its course, for example the Industrial Revolution in the eighteenth and nineteenth centuries. Currently, we are about to embrace what is now termed the Fourth Industrial Revolution, which is characterized by the introduction of artificial intelligence, robotics, more and more interconnection, among other innovations" (World Maritime University, 2019). Nowadays all systems supporting the conduct of navigation and the various IT applications supporting shipping management activities are heavily reliant upon real-time information in order to safely and effectively fulfil their allocated tasks; the issues of connectivity and interconnection are clearly standing out, along with the associated cybersecurity risks.

Modern ships are equipped with numerous highly automated technologically advanced systems. It is no coincidence that modern sea-going vessels have been transformed into "remote offices at sea", with more reliable internet availability. Applications like voice over IP (Internet Protocol), email and instant messaging are now used on-board ships on a daily basis (Dalaklis et al., 2020); recognising that certain cyber risks are also introduced, and introducing the necessary mitigation measures should be viewed as a very high priority action. It is also a self-explanatory fact that the growing digitisation in the maritime logistics domain is one of the driving factors towards the shipping industry's further development. However, it is exactly this expanded use of digital applications that increases the possibility of attacks against information systems.

The professionals participating in the Cyber-MAR training initiatives will have the opportunity to detect attacks on the systems of organisations connected to them, thus being able to protect their systems and avoid cascading effects.

Furthermore, the involvement of various professional figures working in the maritime sector is important, starting with the seafarers that have a vital role to fulfil the mission of "mitigating the various cybersecurity risks"; obtaining the necessary awareness that will allow them to recognise and avoid cyber threats is just the necessary starting point and further training to develop concrete cyber-skills is the next important step. These first/preliminary results that have been previously described are encouraging in terms of willingness to be involved in this challenging issue. Future research efforts will be needed to take full advantage of the results that will stem from the implementation of trainings towards creating maritime professionals that will be equipped with the right skills to be involved in numerous cybersecurity tasks.

## NOTICE

This work is an expanded version of paper presented on Conference DEVPORT 2020: Ports, Transport Maritime et Développement Régional, Le Havre, France, 15 – 16 October 2020.

## REFERENCES

- Alruwaili, A., 2019. A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS. International Journal of Advanced Research in Computer Science, 10(5), pp.1–3. Available at: <http://dx.doi.org/10.26483/ijarcs.v10i5.6476>.
- Blair, J.R.S., Hall, A.O. & Sobieski, E., 2019. Educating Future Multidisciplinary Cybersecurity Teams. Computer, 52(3), pp.58–66. Available at: <http://dx.doi.org/10.1109/mc.2018.2884190>.
- Cabaj, K. et al., 2018. Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, pp.24–35. Available at: <http://dx.doi.org/10.1016/j.cose.2018.01.015>.

- Canepa, M. et al., 2020. Cyber-Security Training Platform on Realistic Maritime Logistics Scenarios, 28th Annual Conference of the International Association of Maritime Economists (IAME), Hong Kong-China (virtual event), 10 June 2020. <http://dx.doi.org/10.13140/RG.2.2.33742.89929>.
- Cyberinsiders, 2019. A brief history of cybersecurity. Available at: <https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/>.
- Cyber-MAR project, 2021. Available at: <https://www.cyber-mar.eu/>.
- Dalaklis, D. and Schröder-Hinrichs, J.U., 2019. The Cyber-Security Element of Hybrid Warfare: Is there a Need to “Formalise” Training Requirements? 10th NMIOTC Annual Conference (“Countering Hybrid Threats: An Emerging Maritime Security Challenge”), Chania-Greece, 4 June 2019. Available at: <http://dx.doi.org/10.13140/RG.2.2.24684.8>.
- Dalaklis, D. et al., 2020. A “Net-Centric” conduct of navigation and ship management. Maritime Technology and Research, 2(2), pp.90–107. Available at: <http://dx.doi.org/10.33175/mtr.2020.227028>.
- De Zan, T., 2019. Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions. Global Cyber Security Center Report. Available at: [https://www.academia.edu/38370900/Mind\\_the\\_Gap\\_The\\_Cyber\\_Security\\_Skills\\_Shortage\\_and\\_Public\\_Policy\\_Interventions](https://www.academia.edu/38370900/Mind_the_Gap_The_Cyber_Security_Skills_Shortage_and_Public_Policy_Interventions).
- De Zan, T., and Di Franco, F., 2019. Cybersecurity skills development in the EU. Heraklion: ENISA. Available at: <https://data.europa.eu/doi/10.2824/525144>.
- European Commission, 2018. Digital education action plan 2018 - 2020. Available at: [https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan\\_en](https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en).
- ISC2, 2019. Strategies for building and growing strong cybersecurity teams - (ISC)<sup>2</sup> cybersecurity workforce study 2019. (ISC)<sup>2</sup>. Available at: <https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482>.
- Kitada, M. et al., 2018. Command of Vessels in the Era of Digitalization. Advances in Human Factors, Business Management and Society, pp.339–350. Available at: [http://dx.doi.org/10.1007/978-3-319-94709-9\\_32](http://dx.doi.org/10.1007/978-3-319-94709-9_32).
- LeClair, J., Abraham, S. & Shih, L., 2013. An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce. Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13. Available at: <http://dx.doi.org/10.1145/2528908.2528923>.
- Rege, A., 2015. Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation. Available at: <https://www.usenix.org/conference/3gse15/summit-program/presentation/rege>.
- Saleh, Y. et al., 2020. Build (don't buy) A skills-based strategy to solve the cybersecurity talent shortage. Available at: <https://www.economicmodeling.com/wp-content/uploads/2020/07/Cybersecurity-BuildDontBuy.pdf>.
- Security, 2020. New research shows US cybersecurity talent shortage. Available at: <https://www.securitymagazine.com/articles/92835-new-research-shows-us-cybersecurity-talent-shortage?v=preview>.
- SentinelOne, 2019. The history of cyber security — everything you ever wanted to know. Available at: <https://www.sentinelone.com/blog/history-of-cyber-security/>.
- Townsend, C., 2019. A brief and incomplete history of cybersecurity. Available at: <https://www.uscybersecurity.net/history/>.
- Tsado, L., 2019. Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach. Journal of Cybersecurity Education, Research and Practice, 2019. Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4>.
- World Maritime University, 2019. Transport 2040: Automation, Technology, Employment - The Future of Work. (Reports 58), Available at: [https://commons.wmu.se/lib\\_reports/58](https://commons.wmu.se/lib_reports/58).