AN INNOVATIVE APPROACH TO PORT MONITORING: DIGITAL TWIN, STRATEGIC DECISION SYSTEMS AND PORT GOVERNANCE

Francescalberto De Bari [(1)], Gianluca Dini [(2, 3)], Giovanni Nardini [(2, 3)], Francesco Papucci [(1)], Matteo Paroli [(1)], Manuela Scarsi [(1)], Ivano Toni [(1)], Mohi-Eldin M. Elsayeh [(4)]

(1) Autorità di Sistema Portuale del Mar Tirreno Settentrionale, Scali Rosciano 6, Livorno, Italia, f.debari@portialtotirreno.it

(2) Polo Universitario "Sistemi Logistici", Università di Pisa, Via dei Pensieri 60, Livorno, Italia

(3) Dipartimento di Ingegneria dell'Informazione, Università di Pisa, Largo Lucio Lazzarino 1, Pisa, Italia

(4) College of Maritime Transport & Technology (CMTT), Arab Academy for Science, Technology & Maritime Transport (AAST&MT), Alexandria, Egypt

Keywords: Digital Twin, Port Monitoring, Cybersecurity, Port Governance.

ABSTRACT

This paper presents an innovative approach to port monitoring systems and highlights the transformative potential of digital twin technology in the dynamic and complex port environment.

To enable a seaport digital twin it is necessary to leverage a "decoupled layers architecture" for port monitoring, emphasizing the importance of an open, scalable, and standard digital architecture. The architecture comprises "on-field components," "communication and connectivity networks" utilizing 5G and Edge Computing, and a "data lake approach" employing a standard microservice architecture.

A significant focus is placed on cybersecurity issues arising from the seaport digital twin, emphasizing the importance of collaborative efforts and regulatory measures. Digital twins are also presented as a tool for simulation and training, allowing the optimization of cybersecurity strategies, especially in the context of IoT-based systems.

The paper concludes by outlining specific functions of digital twins in enhancing innovative port governance, including port development and planning, predictive infrastructure maintenance, environmental monitoring, real-time asset monitoring, security modeling, and operational optimization of port equipment. The proposed "decoupled" approach and the integration of artificial intelligence highlight the potential of digital twins for dynamic and predictive decision-making in seaport management.

1 INTRODUCTION

The port and integrated logistics sector is a complex and interconnected network of people, objects, processes, and technologies. Over time, to optimize efficiency and productivity, different technologies have been tested and consolidated, depending on their different technological maturity [1].

Today, the "digital twin" is a new stage of the evolution of complex information systems. The digital twin technology and approach are still under development in many industries, and from the point of view of the seaports, it represents a very promising frontier [2]. Furthermore, the rapid evolution of artificial intelligence (AI) solutions opens up many opportunities.

Therefore, the frontier consists of the digital twin and AI together as long as these two technologies "enable" each other. In fact, on the one hand, the digital twin feeds artificial intelligence solutions and applications with structured information in real time; on the other, AI assists the digital twin in continuously fine-tuning what, how, how much, and when it is meaningful to project digitally [3].

2 DIGITAL TWIN: CONCEPT AND RELEVANCE TO SEAPORTS

A digital twin is a digital representation or virtual "double" of a physical object, system, or process. As such, the digital twin mirrors the characteristics, behaviour, and dynamics of its real-world counterpart. Digital twins are used in various industries (manufacturing, healthcare, energy, etc.) to monitor, analyse, simulate, control, and optimize the performance of physical entities.

In order to frame the potential of the digital twin for seaports, it is necessary to highlight that it is the physical reality – i.e. the physical object - to determine the characteristics of the digital projection (enabling technologies, potential, strengths and weaknesses, necessary investments). Think of the difference in terms of complexity, not only in technological terms, between the digital projection of:

i. an artefact- i.e., an object conceived and designed by human intelligence (e.g. an airplane, a ship, a container, a port crane, a reach stacker), which incorporates "by design" the sensors and communication systems necessary for monitor and control. It is in this context that the idea of digital twin was first developed and used, for aerospace applications and, in particular, for Product Lifecycle Management;

ii. a complex system of artefacts that interact with each other (e.g.: infrastructures, ships, port equipment that interact with each other in a port; or roads, vehicles, and systems for public services in an urban context);

iii. a natural (non-artefactual) system, whose operating mechanisms are only partially known, and which has large and multiple dimensions. We can think, for example, of the "European Digital Twin Ocean" (European DTO) promoted by European Commission within the framework of the "EU Mission – Restore our oceans and waters by 2023" [4].

Ports are excellent examples of case ii) precisely because they are ideal large-scale real-field testbeds for piloting, prototyping, and demonstration of applications and solutions (including AI) based on the digital twin [5].

Digital twins can play a significant role in seaports to improve efficiency, safety, decision-making, resilience, and sustainability. Before outlining the in-depth functions enabled by digital twins for seaports and port communities, it is necessary to outline the evolution that port monitoring systems have undergone over the years.

3 FROM AN INNOVATIVE APPROACH TO PORT MONITORING TOWARDS THE SEAPORT DIGITAL TWIN

The innovation actions and projects on the digital transition front promoted by the Port Authorities have experienced various phases. The first phase (2012 – 2018) linked to the development of "Port Community Systems" as tools for managing workflows connected to shipping and logistics.

Since 2016, many Port Authorities increasingly focused on creating advanced port monitoring tools.

In the first phase, up until 2019, the port monitoring tools of the Port Authorities were developed in a fragmented way, with the aim to respond to specific monitoring needs (e.g. safety, air quality, dangerous goods). Often, even today, the " on-field components" consist of devices dedicated to

specific functions (cameras, environmental sensors, RFID tags) and are equipped with proper applications and interfaces, which determine a "silo" type data architecture that is very difficult to integrate among each other and which is undoubtedly unsuitable for building a true digital twin.

For Port Authorities, this approach often involves a sort of technological lock-in, deriving from the dependence on specific suppliers and their vertical tools, which ensure the continuity of specific functions but imply the loss of much of the value of the data for the development of new solutions and services [6].

In overcoming this logic, it is possible to operate on two parallel fronts:

i. a profound review of the digital architecture for port monitoring to make it open, scalable, and standardised and to create a sort of "global information space" capable of adequately containing the information set of each individual monitored process;

ii. the development of a general-purpose monitoring system, inspired by the logic of big data and implemented in the cloud with the purpose to collect real-time data from every functional subnetwork of sensors, to integrate data in a structured database, to aggregate these with different information coming from other processes and from other phases of the same process, thus generating new knowledge.

Modern port monitoring must be inspired by the logic of "As A Service" and "Open Data", which should not be interpreted as merely technological or system architecture choices. In fact, the "As A Service" approach allows Port Authorities to resort to the market and extract the best available solutions from it in a fully competitive context. Furthermore, the logic of "Open Data" expresses its full ability to share the added value of the information incorporated in port monitoring systems with users, exposing open interfaces, precisely allowing users to be able to independently develop their own solutions based on the knowledge and value offered by the port monitoring system for which the Port Authority remains responsible as a third-party body.

3.1 "Decoupled Layers Architecture" as enabler of Seaport Digital Twins

In particular, the innovative approach to port monitoring that we propose is based on the decoupling of the different layers involved in monitoring, with the prospect of also enabling automatic control functions for the benefit of the Port Authority and their "extended port communities". The structure of the decoupled layers is shown in figure1:

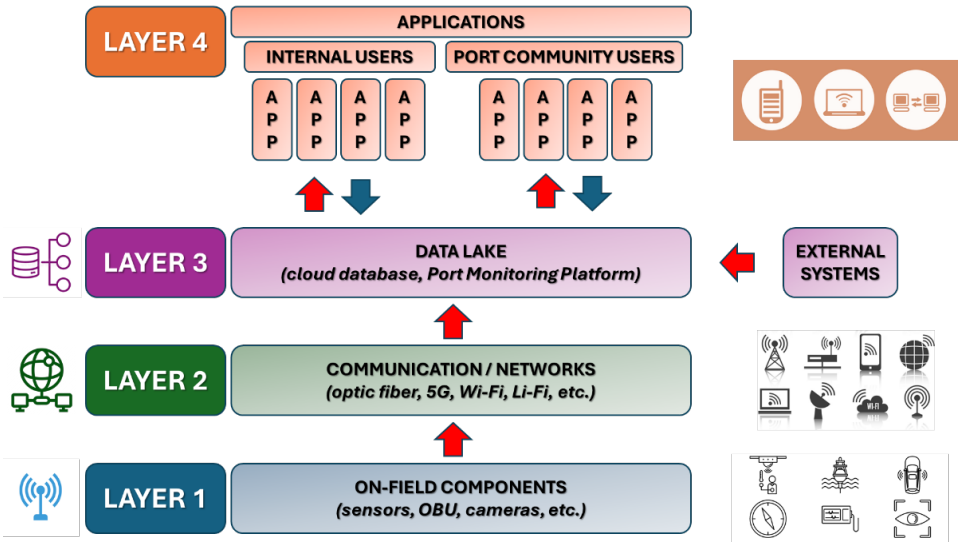

Figure 1: The "decoupled architecture" for Port Monitoring

3.2 Focus on specific Layers of the decoupled architecture

a) "On Field Components". Everything that gravitates inside and outside the seaport can be expressed in the form of "objects": infrastructures, road, rail or naval vehicles, port operations, goods, port facilities, power sources, sensors, and antennas themselves, all of which is connected to the Port. Each object is defined by data attributes and information that characterize it.

The objects, as such, can be related to each other and to the surrounding context by positioning them within a georeferenced system and defining the interactions between them. The same interactions between objects can be specified by data and attributes and, subsequently, the interactions themselves can generate other data as a consequence of the mutual action. In other words, it is the objects themselves, by virtue of existing and "meeting" each other, that generate data automatically and in real- time.

In a nutshell, new generation port monitoring surpasses the "ONCE" paradigm of the "Single Window" [7], in virtue of which each piece of data must be entered only once by the human operator, in the direction of the "NEVER" paradigm, given that no human operator inserts any data. For this to happen, increasingly advanced and distributed sensing is required, which captures the existence of each object with progressively smaller grain size. This process is enabled by the enormous miniaturization, by the improvement of sensors with the most diverse detection functions, often included in the same on-field component and by the vertical collapse of sensor costs due to economies of scale, in the scenario called "fourth industrial revolution" [8].

b) "Communication and connectivity networks": 5G & Edge Computing. The development of a digital twin can include the development of highly innovative solutions that can add value to the twin itself, creating an optimized, more functional, and closer to the concept of "real time" service. For this reason, the networks and communications that innervate the port area are highlighted. Data generated by on-field components represent the "raw material" to build effective port monitoring DTs. Thus, establishing an effective communication layer is crucial to achieving the proposed goal. Implementing a port monitoring DT comes with non-trivial challenges such as the need to collect data from a vast number of heterogeneous devices (i.e., ranging from environmental sensors to autonomous robots and

vehicles), which could have energy constraints, these being often mobile and battery-powered. Moreover, as the DT may need to replicate the system status accurately, real-time requirements must be met by the underlying communication infrastructure.

Wireless technologies commonly used in today's IoT scenarios– such as Wi-Fi and LoRa (Long Range) – fail at providing a comprehensive solution to all the above challenges. Under these circumstances, mobile networks' fifth generation (5G) is the cornerstone of smart and efficient port monitoring [9]. Indeed, 5G was designed to provide differentiated service levels able to support heterogeneous use cases [[10]: besides improving by a factor of ten (as opposed to 4G) the data rate for users exploiting enhanced Mobile Broadband (eMBB) services, 5G implements massive Machine-Type Communication (mMTC) and Ultra Reliable Low Latency Communications (URRLC) capabilities, which support, respectively, up to 1 million connected devices per km2 and communications with less than 1ms of delay and 99.9999% of reliability. MMTC and URLLC are both key for adopting 5G in industry and logistics. Indeed, they match the requirements of a port monitoring DT regarding real-time data transmission from a wide range of devices.

To further meet the requirements of a DT, the adoption of Edge Computing systems is envisaged. The Edge Computing paradigm consists of placing a virtualized computing infrastructure at the network edge (e.g., co-located with the network's access points), hence closer to the end devices – as opposed to Cloud Computing which is instead implemented by remote data centers. The European Telecommunications Standards Institute (ETSI) has standardized the reference architecture for the Multi-access Edge Computing (MEC) system [11], aiming at realizing an open virtualized platform where (third-party) developers can use standard Application Programming Interfaces (APIs) to instantiate their applications on the MEC provider's computing infrastructure. Moreover, due to the natural integration between ETSI MEC and the 5G network, applications can be made aware of the local context they operate in by capitalizing standardized APIs in order to gather useful information from the underlying 5G network itself , e.g., the geographical location of devices [12]. By instantiating the DT itself at MEC nodes, context-aware DT applications can be flexibly implemented while reducing the latency of data coming from IoT devices and meeting DTs' real-time requirements.

c) "Data lake approach": Standard Microservice Architecture. As mentioned, the development of a digital platform cannot beintendedas a predefined, predictable, and closed process, especially in a continuously evolving system and in constant search for innovative solutions with high added value. This leads to implement systems with different methodologies and designs, which accommodate the needs and requests of individual interested parties, both on the back-end and front-end side.

The decoupling between platform and applications can be achieved through a "microservices" architecture, which allows a more streamlined process. This would guarantee the development of timely solutions capable of responding to the needs of any requesting party. The resulting "data lake" allows:

- insertion of structured and unstructured data;
- scalable data storage and protection;
- catalogs and indexes without the need to move data;
- data virtualization and connection to accredited third-party applications via transparent APIs.

Through access to the data lake, it is possible to create a virtual real-time instance of the system ports, their status, the events that have been detected, the risk status around some functions, situations, etc.

Finally, it will be more relevant to point out that innovative solutions, applications and tools (such as AI or Cooperative Intelligent Transport Systems) can be framed starting from this reference architecture for port monitoring.

4 CYBERSECURITY ISSUES ARISING FROM THE SEAPORT DIGITAL TWIN

Nowadays, the digital transformation that smart ports are experiencing constitutes the main driver of change in the port sector. The increasing integration of diverse devices, agents, and operations, along with the increasingly tight interactions among ports, have created a new ecosystem that paves the way towards innovations such as towards new threats and risks [13]. In this scenario, cybersecurity emerges as a pivotal challenge that necessitates collaborative efforts between all port stakeholders to protect these critical infrastructures while deploying the new 4.0/5.0 technologies in a sector that has relatively lagged in the digital transition process until now [14].

Cybersecurity is considered one of the three main risks at ports, together with piracy and submersible security [15]. However, many ports are not yet fully prepared to face the cyber risk [16]. Cyber-attacks on ports are not a hypothetical or theoretical risk but are a reality. In recent years, cyberattacks on ports and shipping have become more common. For instance, in February 2022, several European ports were hit by a cyberattack that disrupted oil terminals [17]. Furthermore in January 2023, the Port of Lisbon was targeted by a ransomware attack that threatened the release of port data [18]. In November 2023, major Australian ports shut down due to a cyber-attack impacting the movement of goods in and out of the country [19].

Effectively managing cybersecurity risk requires actions along several dimensions. On a normative dimension, for example, the European Union issued the Network and Information Systems (NIS) Directive (EU Directive 2016/1148) - and its revised version Directive known as NIS2 (EU Directive 2022/2555) - a piece of EU-wide cyber security legislation that aims to achieve a high-level of network and information system security shared across all the EU's critical infrastructures (e.g., ports).Furthermore, many shipping companies along with other organizations, have published guidelines and recommendations specifically designed for this industry. For instance, in 2019 the European Network and Information Security Agency (ENISA) published a guide on Port Cybersecurity listing good practices in the maritime sector [20]. Most recently, the International Maritime Organization (IMO) published guidelines on maritime cyber risk management [21].

On an organizational dimension, according to IMO, there is an urgent need to raise awareness and preparedness of the port and maritime sector on cyber-risk threats and vulnerabilities to support safe and secure shipping [22]. Ship owners, shipping agents and port authorities may have adequate resources to procure cybersecurity technologies and to take adequate organizational measures, yet the question that arises is about the galaxy of small-medium enterprises (SMEs) that revolve around ports: Due to the fact that cybersecurity attacks on SMEs do not always make headlines, SMEs often tend to underestimate their vulnerability and underinvest in security. However, adversaries have something to gain from just about any business and thus SMEs face many of the same threats as enterprises. In addition to the value of their data, in a lateral movement strategy, SMEs that work with large enterprises may be attractive intermediate objectives towards bigger businesses. In this case, the loss may derive from the termination or non-renewal of a supply contract.

Finally, on a technological dimension, while the Internet of Things (IoT) is the key enabling technology for smart ports, at the same time, IoT devices are growing into the new weakest link in the security chain in the modern ports and are becoming a powerful amplifying platform for cyberattacks. Therefore, IoT cybersecurity must not be an afterthought when developing and using IoT devices.

Several threats and possible countermeasures have already been identified for IoT-based systems [23]. However, recently, digital twins have emerged as a viable and effective technology to face cybersecurity in cyber-physical systems. A digital twin is a high-fidelity digital model of a physical system or asset that could be used, e.g., to optimize operations and predict faults of the

physical system. While digital twins are considered as one of the top technological trends, and even more industries are looking into the usability of this technology to optimize the development and maintenance of their systems and processes, very little is known about using digital twins for cybersecurity.

Digital twins may have two primary employments for cybersecurity, namely simulation and training. Digital twins allow us to simulate an attack on a cyber-physical asset, providing information about system weaknesses and behavior under attack. Simulations enable repeatability and offer to compress the time interval. Additionally, simulations, possibly enriched by data analytics and machine learning, can illustrate and predict a system's behavior under a broad range of specified configurations such as during a security incident that supports the comprehension of emergent as well as prospective behavior. Most importantly, simulations run in a standalone virtual environment and therefore, do not affect the physical environment. Moreover, whenever historical data is missing, resulting data of simulations may deliver important input.

Modeled on the physical shooting ranges used by police and the military, a cyber range creates a training space that simulates a wide range of security incidents so cybersecurity professionals can practice and learn how to respond effectively. Building a cyber range for a cyber-physical system requires the reproduction of industrial scenarios to support offensive and defensive. However, building an IoT-based cyber range encounters two challenges. First, the industrial field devices on the cyber range are expensive and difficult to deploy and have poor reproducibility, so every construction of an IoT-based cyber range requires the repeated purchase of industrial field devices and the experts to deploy and install them, which is a waste of resources both in finance and energy. Second, during the use of the cyber range, if network attacks cause damage to the industrial site, scenario restoration will often be time consuming, which restricts the efficiency of the cyber ranges to a high degree.

Digital Twins have the potential to win these challenges [24]. On the one hand, digital twins can substitute real devices to react to attacks from cyber ranges to avoid unnecessary damages due to their financial value. On the other hand, in order to deploy cyber ranges freely without the limitations of the devices or locations, a digital twin-based cyber range is ideally a promising approach. Despite all these benefits, up until now, simulations and training based on digital twins have been largely neglected in current cybersecurity approaches.

5 SPECIFIC DIGITAL TWIN FUNCTIONS FOR INNOVATIVE PORT GOVERNANCE

From a Port Authority point of view, the main strategic and operational functions of the digital twin are the following:

a) Port development and planning. Digital twins help in planning and expansion of port infrastructure. Port authorities can simulate the impact of new developments, expansions or changes in operations before implementing them in the physical environment, ensuring optimal use of resources. In particular, to improve the decision-making process, it could be helpful to simulate several scenarios for the development of the infrastructure. From this point of view, the digital twin is a "Strategic Decision Support System" [25].

b) Predictive infrastructure maintenance. Digital twins enable predictive maintenance, continuously monitoring the evolving condition of equipment and infrastructure. This helps to identify potential problems prior to failure, reducing downtime and maintenance costs. In this regard, consider the predictive maintenance of the seabed through dredging operations.

c) Environmental monitoring: Port operations always have environmental impacts. Digital twins can incorporate environmental monitoring systems to assess the impact of port activities on air and water quality, allowing authorities to implement measures for sustainable and environmentally friendly operations.
d) Monitoring, management, and control. Digital twins enable real-time monitoring of physical assets such as cranes, containers, ships and other infrastructure and spaces within the port [26]. Monitoring facilitates better management of resources both for Port Authorities and terminal operators, also through the remote control of assets and facilities. These functions, enabled by the digital twin, are particularly important for multipurpose ports and for seaports in which a multiplicity of operators use the same assets and infrastructures (berths; gates; short, medium and long-term parking areas; disengagement areas for ferries and cruise passenger flows; energy supply points, also given the activation of OPS systems). From a long-term perspective, the advanced digital twin could pave the way for the "co-use" of the spaces where port operations occur [27].
e) Security. Digital twins can be used to model and simulate security scenarios, helping port authorities plan security and emergency response measures, which include monitoring and controlling access to sensitive areas and responding to potential security threats.
f) Operational optimization of port equipment. By creating a digital double of the entire port environment and allowing access to the data lake in real-time, Port Authorities enable terminal operators and authorized companies to optimize port operations, with additional benefits from an environmental point of view and the safety of workers and users of the system [28].

6 CONCLUSIONS

In the decoupled architecture proposed above, the digital twin finds connection with the solutions/applications layer; foremost, what needs to be pointed out is that the real-time data flow between physical and digital twins requires the use of different technologies enablers, such as artificial intelligence, augmented reality, virtual simulations, big data & analytics and the Internet of Things (IoT). In particular, the importance of the "digital twin - artificial intelligence - IoT" triptych emerges: the IoT detects an "event" through a device, after which object, event and device are represented on the digital model of the port; therefore, the application of AI allows the information received to be correctly processed and analysed, integrating it with others, especially in predictive terms.

In conclusion the decoupling of the layers is to be considered one of the leading solutions also for the implementation of a digital twin that represents a digital projection of the seaport in a dynamic way, drawing on data from heterogeneous sources.

ACKNOWLEDGMENTS

This work has been financed by the European Union—NextGenerationEU (National Sustainable Mobility Center CN00000023, Italian Ministry of University and Research Decree n. 1033 - 17/06/2022, Spoke 10).

REFERENCES

[1] T. Inkinen, R. Helminen, J. Saarikoski, "Technological trajectories and scenarios in seaport digitalization". *Research in Transportation Business & Management*, vol. no. 41 (2021). https://doi.org/10.1016/j.rtbm.2021.100633

[2] R. Klar, A. Fredriksson and V. Angelakis, "Assessing the Maturity of Digital Twinning Solutions for Ports". *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, Atlanta, USA (2023): 552-557. https://doi.org/10.1109/PerComWorkshops56833.2023.10150378
[3] J. Neugebauer, L. Heilig, S. Voß, "Digital Twins in Seaports: Current and Future Applications". *Lecture Notes in Computer Science*, vol no. 14239 (2023). https://doi.org/10.1007/978-3-031-43612-3_12
[4] European Commission, *European Mission - Restore our Oceans and Waters by 2030. Implementation Plan*, 2021.
[5] R. Klar, A. Fredriksson and V. Angelakis, "Digital Twins for Ports: Derived From Smart City and Supply Chain Twinning Experience". *IEEE Access*, vol. no. 11 (2023): 71777-71799. https://doi.org/10.1109/ACCESS.2023.3295495
[6] K. Wang et al., "Multi-aspect applications and development challenges of digital twin-driven management in global smart ports". *Case Studies on Transport Policy*, vol. no. 9, Part 3 (2021). https://doi.org/10.1016/j.cstp.2021.06.014
[7] United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), Recommendation and Guidelines on establishing a Single Window, Recommendation n. 33, 2005.
[8] K. Schwab, "Fourth Industrial Revolution". Penguin Book (2019).
[9] R. Du, A. Mahmood and G. Auer, "Realizing 5G smart-port use cases with a digital twin," in *Ericsson* Technology Review, vol. 2022, no. 13, pp. 2-11, December 2022, doi: 10.23919/ETR.2022.9985778
[10] O. O. Erunkulu, A. M. Zungeru, C. K. Lebekwe, M. Mosalaosi and J. M. Chuma, "5G Mobile Communication Applications: A Survey and Comparison of Use Cases," in *IEEE Access*, vol. 9, pp. 97251-97295, 2021, doi: 10.1109/ACCESS.2021.3093213
[11] ETSI GS MEC 003, v3.1.1, "Multi-access Edge Computing (MEC); Framework and reference architecture", March 2022.
[12] ETSI GS MEC 013, v3.1.1, "Multi-access Edge Computing (MEC); Location API", January 2023.
[13] I. Ashraf et al., "A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry", in *IEEE Transactions on Intelligent Transportation Systems*, no. 24-2 (2023): 2677-2690. doi: 10.1109/TITS.2022.3164678
[14] de la Peña Zarzuelo I. "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue." *Transport Policy*, no.100 (2021): 1-4. https://doi.org/10.1016/j.tranpol.2020.10.001
[15] Deep Trekker, 2020. *Top 3 risks at our ports*. Retrieved on 23-12-2023. https://www.deeptrekker.com/resources/maritime-port-security-risks
[16] Schauer, S., Polemi, N., and Mouratidis, H., 2019. "MITIGATE: a dynamic supply chain cyber risk assessment methodology." *Journal of Transportation Security* no. 12 (2020): 1–35. https://doi.org/10.1007/S12198-018-0195-Z
[17] EuroNews. *Oil terminals disrupted after European ports hit by cyberattack*. 2022. Retrieved on 23-12-2023. https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack
[18] The Maritime Executive. *Cyberattack Threatens Release of Port of Lisbon Data*. 2022. Retrieved on 23-12-2023. https://maritime-executive.com/article/cyberattack-threatens-release-of-port-of-lisbon-data
[19] Samira Sarraf. "Major Australian ports shut down following cyber incident." CSO, 2023. Retrieved on 23-12-2023. https://www.csoonline.com/article/1246710/major-australian-ports-shut-down-following-cyber-incident.html
[20] Drougkas, A., Sarri, A., Kyranoudi, P., Zisi, A., 2019. Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector. Technical Report. European Network and Information Security Agency (ENISA). Retrieved on 23-12-2023. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sec
[21] IMO. *Guidelines on Maritime Cyber Risk Management*. IMO Circular MSC-FAL.1/Circ.3, 2017.
[22] IMO. *Maritime Cyber Risk Management In Safety Management Systems*. IMO Resolution MSC.428-98/2017.

[23] Swessi, D., Idoudi, H. "A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures." Wireless Personal Communication no. 124 (2022): 1557–1592. https://doi.org/10.1007/s11277-021-09420-0

[24] Becue A. et al. "CyberFactory#1—Securing the industry 4.0 with cyber-ranges and digital twins" in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst.*, pp. 1–4, 2018. doi: 10.1109/WFCS.2018.8402377

[25] C. Zhou et al, "Analytics with digital-twinning: A decision support system for maintaining a resilient port". *Decision Support Systems*, vol. no. 143 (2021). https://doi.org/10.1016/j.dss.2021.113496

[26] F. De Bari, F. Papucci, M. Paroli, M. Scarsi, I. Toni, "Navigating the future: analysing the effects of autonomous ships on mediterranean port operations and management". *PIANC Med Days and Port of the Future Conference*, Sète, France (2023)

[27] W. Hofmann, F. Branding, "Implementation of an IoT- and Cloud-based Digital Twin for Real-Time Decision Support in Port Operations". *IFAC-PapersOnLine*, vol. no. 52, issue 13 (2019). https://doi.org/10.1016/j.ifacol.2019.11.516

[28] F. De Bari et al., "Addressing Efficiency and Sustainability in the Port of the Future with 5G: The Experience of the Livorno Port. A methodological insight to measure innovation technologies' benefits on port operations". *Sustainability*, vol. no. 13/2021