Review of Management and Economic Engineering
Vol. 23, Nr. 2(92), June 2024, p. 113 - 121, ISSN (print): 1583-624X, ISSN (online): 2360-2155

ENVIRONMENTAL CONCERNS AND CYBER SECURITY. WHAT DO THEY HAVE IN COMMON IN THE PORT ACTIVITY?

Andreea-Maria MOLDOVEANU[1], Aurel-Mihail ȚÎȚU[2,3*]

1 *National University of Science and Technology POLITEHNICA Bucharest, Faculty of Industrial Engineering and Robotics, 313 Splaiul Independenţei, 6th District, Bucharest, Romania, e-mail: andreea.ungureanu1397@gmail.com*

2 *Lucian Blaga University of Sibiu, 10 Victoriei Street, Sibiu, Romania, mihail.titu@ulbsibiu.ro,*

* *Correspondence: mihail.titu@ulbsibiu.ro*

Abstract: In the context of sustainable development and the achievement of European and global carbon footprint reduction goals, ports have an essential aim in the balance between global warming and sustainable development. Moreover, digitalization and the fast evolution of IT facilitate the infiltration of vulnerabilities in port systems that can lead to negative events, the issue of cyber security thus becoming a concept present in all structures of the logistics supply chain. This paper shows the implications of the deficiencies of one aspect over the other in the port field and how the integrated approach of the two concerns facilitates the green transition of ports in a safe and secure environment.

Keywords: sustainable development, cyber security, port system, green transition, cyber attacks

1 INTRODUCTION

Currently, two critical areas are under intense global scrutiny. One is sustainable development in the face of global warming, leading to the adoption of numerous international environmental policies and objectives (United Nations, 2015). The other is cyber security, which addresses the protection of network and IT systems amid rapid technological advancement and digitization. Given their global importance, it is essential to integrate these concerns into all critical infrastructures, including sea ports, which are fortunately under thorough examination and debate.

However, despite sustainable development and cyber security being crucial for the development and enhancement of port activities, they are seldom discussed together. This oversight can lead to vulnerabilities that compromise both environmental and technological aspects of port operations. The interconnected nature of modern port activities means that a breach in cyber security could have significant environmental consequences, while poor sustainable practices can exacerbate security risks. This paper aims to address this gap, highlighting the need for an integrated approach to port management that encompasses both sustainable development

and cyber security. By examining case studies, current policies, and emerging trends, this paper seeks to provide a framework for policymakers and industry stakeholders to enhance port resilience and sustainability in tandem.

2 BACKGROUND

As a major player in global transportation and commerce, maritime transport currently accounts for 80% of the total volume of goods traded worldwide (United Nations, 2019). Ports serve as the crucial interface between water and land freight transport, but they also contribute significantly to air pollutant emissions due to the handling and transportation of freight to and from the port.

The port and maritime sector has reached its actual stage through notable increase over the past twenty years. The capacity of the global container fleet has expanded six times since 1990 (Tran & Haasis, 2015). Due to its cost advantage, shipping is regarded as the primary and most environmentally friendly mode of international freight transport worldwide. For instance, the European Union targets to shift 30% of its freight transport, covering distances greater than 300 km, from road transport to either rail or maritime transport (Rødseth, Schøyen, & Wangsness, 2020).

However, it has been verified that maritime transport has a significant contribution on air pollution, particularly in coastal regions, while it is indispensable to global socio-economic advancement (Wild, 2021). Hence, due to the substantial expansion of international shipping in recent decades, emissions from shipping and ports, along with their associated impacts, have garnered heightened attention worldwide (European Commission, 2022). Additionally, recent research systematically correlates air pollution with adverse health outcomes among affected populations (Cai, Peng, & Yu, 2021).

In the Paris Agreement (Consiliul Uniunii Europene, 2016) there are targets to control the rise in global average temperature. It appears improbable that these goals will be met by the year 2100, while around 2.4% of global anthropogenic emissions, that are expected to grow in the next decades, are generated by global transport. Lately, there has been significant pressure on ports and maritime transport industry to decrease their greenhouse gas emissions. Moreover, shipping is anticipated to be one of the rapidly expanding industries in terms of greenhouse gas emissions (Cai, Peng, & Yu, 2021).

Cyber security is a major concern in the digital age we live in. Moreover, in the port field, securing networks and information systems becomes a priority considering the huge amount of information and technology rapid development (Bunyamin, Gizem & Pelin, 2021). On the one hand, it facilitates the increase in productivity and effectiveness of port activities integrated in the entire logistics chain, but on the other hand, it creates the environment conducive to the development of large vulnerabilities, namely opportunities for malicious entities. Ports are critical points in the global flow of the logistics chain that require adequate protection against cyber threats (Akpan et al, 2022).

Cyber attacks directly affect the normal development and optimization of processes in a port (ENISA, 2021). These can be of a nature to affect the computer system by producing blockages with the aim of obtaining money, or they can be of a terrorist type, with the aim of causing material and human damage, environmental impact, disasters, etc. (Avanesova et al, 2021).

There are activities and threats that continue to represent significant challenges that can address various areas, especially seaside areas and also far EU territories which are more at risk. These activities are represented by threats or illegal actions like piracy, offshore armed robbery, organized crime, terrorism, arms and drug trade, illegal, unreported and

unregulated fishing, the presence of undetonated munition in the marine environment. There is a possibility that poor port security facilitates some of these illicit activities (European Commission, 2023).

Some of the most famous maritime cyber security events are the cases: Maersk (Industrial Cybersecurity Pulse, 2021) which was affected by the NotPetya virus that was able to attack Maersk's global network because it was uploaded to a single unprotected computer but which was connected to the company's global network, which caused the contamination of the entire system; and COSCO Shipping (COSCO Shipping, 2023) which experienced a Ransomware attack - the incident shut down the transporter's phone and email services to customers, which required an immediate action plan.

The port industry, like many other sectors, is experiencing digital advancements, resulting in a rise in potential vulnerabilities. Criminals are increasingly using hybrid and cyber techniques to target maritime facilities, including ports, ships, and even submarine pipelines and wires.

Recommendations of the European Union Council on a coordinated approach at Union level to enhance the resilience of critical infrastructure recognizes the call for action. In addition, the Recommendation on the Union's disaster resilience objectives proposes means that may help to increase European readiness and response capacity to natural and human-generated catastrophes, including in the maritime environment (European Commission, 2023).

Since the inception of the European Union's Maritime Security Strategy in 2014, numerous shifts in the global geopolitical landscape necessitate fresh and reinforced measures. The comprehensive threat assessment across the EU indicates a surge in threats and challenges, particularly within the maritime sphere. There's a noticeable uptick in strategic "fight" for resources and power (Alcaide & Llave, 2020).

Menaces are evolving into intricate and many forms, certain nations endeavouring to redefine fundamental principles of the multilateral order, often by encroaching upon national sovereignty and borders.

The military hostility of Russia towards Ukraine has rekindled warfare in Europe, ushering in new perils and adverse ramifications on European maritime security, environmental integrity, and economic stability, thereby impacting European citizens and enterprises (Ben Farah et al, 2022). Maritime security encounters various challenges across numerous regions, encompassing territorial and disagreements, rivalry for natural resources, and infringements upon free navigation as well as the rights for transit. These confrontations breed pressures within sea basins neighboring the European Union, notably in the Mediterranean Sea, Black Sea, Baltic Sea, further boosted by the war in Eastern Europe (European Commission, 2023).

Have we ever wondered if, in addition to the risks to which critical electronic systems are subjected, cyber threats can also have environmental consequences in the functionality of the port? But vice versa?

3 METHODOLOGY

The authors addressed two highly debated themes worldwide applied in one of the important sectors in the functioning of society, namely the port field. Studying the two subjects separately reveals an extraordinary scientific activity.

For a literature synthesis in the addressed field, Clarivate Analytics' Web of Science (WoS) platform was used to search for the most relevant articles. For the topic on the environment, we proceeded to search for articles that contain the key words in the "topic" field: "environment" and "port". The selected period was 2014-2024 to see the status in the last 10 years. 6,462 items matching the selections were

identified. If we had replaced the word "port" with "seaport", the list of results would have been narrower with a number of 335 results. For the field of cyber security, the keywords selected were: "cybersecurity" and "port", the selected time period being the same as the last 10 years. A number of 117 relevant articles were identified. If we had replaced the word "cybersecurity" with "security", we would have obtained a number of 6,462 articles, but we were strictly interested in cyber security.

When we merged the keywords into a single search ("port", "environment", "cybersecurity") we obtained a number of 23 articles, the most recent of which are from the last four years. From here we understand that the approach to the two aspects simultaneously in the port sector was reduced. We believe that this number could increase in the next period, considering that some aspects of one sector may have important implications on the other sector in terms of the functionality of the port.

Dependence on technology and, more recently, the introduction of artificial intelligence into all organizational structures comes with many challenges today. The field of cyber security is among the main topics discussed worldwide due to the increasing need to maintain the safety of critical infrastructures at the expense of emerging threats that we face at every step. The relevant authorities, research centers, international organizations (e.g. European Cybersecurity Competence Centre, European Security and Defence College, International Maritime Organization, European Cyber Security Organisation The European Union Agency for Cybersecurity) promote and share through all media sources, but also through scientific events (e.g. the series of the Black Sea Cybersecurity Conference), good practices and research results in order to improve the quality and safety of citizens' lives in the current context.

Furthermore, we are in the "era" of sustainability, of the green transition towards a cleaner world with reduced carbon emissions in the context of global warming. At the global level, this concern is the order of the day in every organization. Ports represent important logistical nodes in the supply chain, with an impressive activity that can involve the generation of greenhouse gas emissions, various types of pollution, etc.

4 APPROACH

In order to carry out this study, the most relevant official documents in the addressed fields and also the most relevant articles were documented.

- Paris Agreement (Official Journal of the European Union, 2016) - 1.5˚C scenarios (Allen et al, 2018);
- The 2030 Agenda for Sustainable Development (United Nations, 2015);
- Fit for 55 - European Green Deal (European Commission, 2023);
- European Climate Law 2021 (Official Journal of the European Union, 2021);
- 2023 IMO Strategy on Reduction of GHG Emissions from Ships (IMO, 2023);
- (The European Scientific Advisory Board on Climate Change, 2023);
- SOLAS XI-2 and the ISPS Code. (IMO, 2014);
- Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the regions European Climate Pact (European Commission, 2020);
- Joint communication to the European Parliament and the Council. An update of the EU Maritime Security Strategy and its Action Plan (European Commission, 2023).

This paper aims to look up on how security issues can impact environmental management and sustainable development in ports. It also seeks to illustrate how some environmental factors can affect the security and safety of

critical infrastructure, including ports, highlighting the need for increased awareness among national and local decision-makers.

The relationship between cyber security and port environmental concerns is intricate and mutually reliant. Vulnerabilities introduced in one aspect can result in severe repercussions for the other, and vice versa.

Apart from human threat actors, port systems face environmental threats stemming from natural occurrences such as solar events, weather phenomena, animals, and insects. These factors can induce damage, malfunction, or substantial harm to port utilities and systems. In extreme cases, port data may be compromised or lost (The Institution of Engineering and Technology, 2020).

An illustration of the impact of natural occurrences on port operations might be considered the high tide event on December 5, 2013, which affected the port of Immingham (Spencer, Brooks, Evans, Tempest, & Möller, 2015). This incident resulted in millions of tonnes of seawater surging over the lock gates into the port. Immingham, renowned as Britain's busiest cargo port, remained submerged for several weeks. The port boasted a network comprising over 40 electricity substations, nearly half of which suffered varying degrees of water damage, with ten substations severely affected. These substations are crucial for supplying electricity to port systems, but due to the damage inflicted upon the port's power infrastructure, operations came to a halt. Sump pumps, essential for regulating water levels in the docks, were submerged underground and rendered inoperable. Engines and equipment had to undergo dismantling for repair or replacement.

Moreover, as climate change affects and will continue to affect many sectors in the medium and long term, these, together with marine pollution, are expected to have important negative effects on maritime security as well.

These impacts include coastal and island flooding, the decline of coral reefs, mangroves, and other wetlands, as well as the depletion of fish populations. These environmental changes act as catalysts for increased insecurity, heightening vulnerability and lawlessness, amplifying transnational criminal activities, piracy, and straining marine resources. As a result, there is a need for a new approach that allows the European Union to enhance societal resilience against climate change, protect the environment, and reverse the trend of ecosystem degradation.

Concurrently, deficiencies in the security of maritime industry could occur in ecological harm, like hindering the access to polluted areas, diverting funds earmarked for environmental preservation, sabotage actions targeting critical infrastructure like the ports. Additionally, the current war has inflicted not only huge human, material and financial losses, but also a notable depletion of biodiversity (ENISA, 2023).

Hence, it is imperative to tackle the interplay among climate change, coastal and marine environment, and maritime security, incorporating both current and novel studies (European Commission, 2023). Figure 1 shows the relationship of interdependence between cyber security management and environmental management when it comes to maintaining and increasing the efficiency of the port system, the relationship between the two having a direct effect on it.

A seaport constitutes a multifaceted information environment encompassing both land and costal activities.

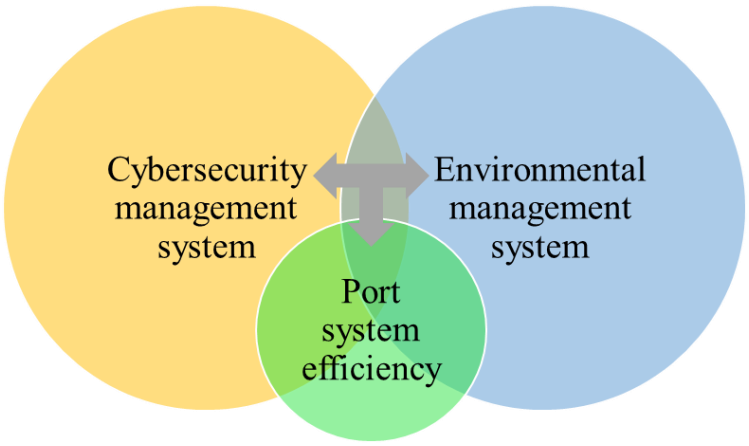

Figure 1. The relationship between cyber security and environmental concerns in increasing the efficiency of the port system

Typically, a port comprises four primary asset categories (these are buildings, linear infrastructure, plant and machinery, and information and communication systems) utilized to deliver a variety of operational services, with technology assuming an increasingly pivotal role. The loss or compromise of any of these assets holds the potential to impact the following aspects (The Institution of Engineering and Technology, 2020):

- Speed and efficiency of port operations;
- Port's capability to conduct specific operations safely;
- Health and safety of personnel and other individuals affected by the conducted work activities, to whom a duty of care is owed.

To this list of aspects that can be affected by the compromise of one or more assets, we could add "the environment", where different environmental aspects can be generated and which can have consequences on the environmental factors that are present in the port such as: water, soil, air, marine environment.

An instance of compromising one of the four outlined assets, such as communication and information systems, might involve attacking guidance systems, ship piloting, or other communication systems (Jones, 2015) like Global Navigation Satellite System (GNSS), as well as the Global Positioning Satellite (GPS) (Zarzuelo, 2021). Such threats could result in maritime accidents, leading to material losses, delays, and financial setbacks and the obstruction of channels. But, these incidents may cause spills or leaks from fuel or oil tanks, potentially resulting in irreparable environmental disasters.

5 CONCLUSION

A safe future in the port field and throughout the logistics chain, in today's context, of rapid IT development and the implications of climate change, is represented by the maintenance and optimization of the level of cyber security and the growth and fruition of environmental concerns.

This must be achieved at a global level, starting from the port organizations through the implementation of integrated management systems likely to accelerate the achievement of these objectives by applying techniques and methods for evaluating organizational performance and continuous optimization of activities and processes, from the simplest daily activities to the most complex ones.

The current international context, generated by the crisis in Ukraine, has led to the reorientation of the flows of goods through Romanian ports and to the increase in the traffic of goods which, in certain situations, has led to the appearance of blockages in terms of the handling/transshipment/operation of goods

The geopolitically uncertain period that we are going through fuels and potentiates cyber and environmental threats at the port level.

Although it is seldom discussed, the war in Ukraine has a significant environmental impact not only there but also in neighboring countries. Romania, in particular, is vulnerable. Every day the conflict continues, there is an increased risk of dangerous substances contaminating the water, food, and air, spreading from the neighboring front.

Residues from munitions, explosions, mechanical destruction from military machinery and vehicles, wildfires, acid rain, and the release of various toxic substances all severely affect the soil, water, and air.

On the other hand, propaganda, fake news and mass manipulation in all social media and cyber attacks can contribute to the generation of even greater conflicts, having negative consequences on the functionality of the ports.

Therefore, when the potential risks are taken into account, they could be addressed both from the point of view of the potential impact on the port and neighboring environment, but also of port cyber security.

That is why, when the potential risks are taken into account, they could be approached both from the point of view of the potential impact on the port and neighboring environment, but also of port cyber security. Useful results might be obtained when evaluating the risks associated with: intrusion attempts, preparedness level, access management, security incidents together with pollution level, waste, energy efficiency, environmental issues.

The risks become even greater with the automation of many processes, port facilities and the introduction of more and more autonomous ships, where the infiltration of vulnerabilities in electronic and monitoring systems is much more targeted. These innovations can also influence the response time in taking immediate actions after noticing the materialization of an environmental or security risk.

The establishment of legislative frameworks for reporting environmental performance, carbon footprint and cyber security issues contributes to increasing the degree of organizational awareness that will generate new national and international policies and methodologies or the updating of existing ones for the purpose of sustainable development and cyber safety aligned to global goals (DNV, 2023).

Future analyzes and studies may identify the need for investment in existing port infrastructure and superstructure or the development of new ones, investment in the existing aging fleet, in services that take into account strict conditions in terms of energy and the technologies and information systems used, including aspects related to Artificial Intelligence and the development of a Port Community System.

Also, increasing the number of cyber security exercises in the maritime field to address the environmental implications in the affected area, in addition to the operational blockages generated will increase the degree of knowledge, good practices, preparedness and quick response to possible cyber security and environmental incidents.

BIBLIOGRAPHY

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123–138. https://doi.org/10.3390/network2010009

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Allen, M.R., O.P. Dube, W. Solecki, F. Aragón-Durand, W. Cramer, S. Humphreys, M. Kainuma, J. Kala, N. Mahowald, Y. Mulugetta, R. Perez, M. Wairiu, and K. Zickfeld, 2018: Framing and Context. In: Global Warming of 1.5°C. An IPCC Special Report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty [Masson-Delmotte, V., P. Zhai, H.-O. Pörtner, D. Roberts, J. Skea, P.R. Shukla, A. Pirani, W. Moufouma-Okia, C. Péan, R. Pidcock, S. Connors, J.B.R. Matthews, Y. Chen, X. Zhou, M.I. Gomis, E. Lonnoy, T. Maycock, M. Tignor, and T. Waterfield (eds.)]. Cambridge University Press, Cambridge, UK and New York, NY, USA, pp. 49-92, doi:10.1017/9781009157940.003.

Avanesova, T. P., Gruzdeva, L. K., Iuskaev, R. A., Gruzdev, D. Y., & Somko, M. L. (2021). Analysis of cyber-security aspects both ashore and at sea. IOP Conference Series: Earth and Environmental Science, 872(1), 012024. doi:10.1088/1755-1315/872/1/012024

Ben Farah, M., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber-Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information, 13(1), 22. doi:https://doi.org/10.3390/info13010022

Bunyamin, G., Gizem, K., & Pelin, B. (2021). Cyber security risk assessment for seaports: A case study of a Container port. Cyber&Security Journal. doi:10.1016/j.cose.2021.102196

Cai, O., Peng, C., & Yu, X. (2021). The development of port emissions inventory from decision-making perspective: case of the port of Los Angeles. IOP Conference Series: Earth and Environmental Science, 012022. doi:10.1088/1755-1315/675/1/012022

European Commission. (2023, 3 10). An enhanced EU Maritime Security Strategy for evolving maritime threats. Bruxelles. https://eur-lex.europa.eu/resource.html?uri=cellar:9e3d4557-bf39-11ed-8912-01aa75ed71a1.0001.02/DOC_1&format=PDF

Consiliul Uniunii Europene. (2016, 10 5). DECIZIA (UE) 2016/1841 A CONSILIULUI. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016D1841

COSCO Shipping. (2023). COSCO Shipping. https://lines.coscoshipping.com/home

DNV. (2023). Energy Transition Outlook - Maritime Forecast 2050. A deep dive into shipping's decarbonization journey.

European Commission. (2020). Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the regions. European Climate Pact. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A788%3AFIN

European Commission. (2022). Accelerating the transition to climate neutrality for Europe's security and prosperity, Climate Action – Progress Report 2022,. Retrieved from https://climate.ec.europa.eu/system/files/2022-12/com_2022_514_web_en.pdf, Bruxelles

European Commission. (2023). A European Green Deal. Retrieved from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en

European Commission. (2023). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the update of the EU Maritime Security Strategy and its Action Plan "An enhanced EU Maritime Security Strategy for evolving maritime threats". Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0008

ENISA. (2021). Understanding the increase in Supply Chain Security Attacks. Retrieved from https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

ENISA. (2023). IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030. doi:https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030/@@download/fullReport

IMO. (2023). 2023 IMO STRATEGY ON REDUCTION OF GHG EMISSIONS FROM SHIPS. Retrieved from https://wwwcdn.imo.org/localresources/en/OurWork/Environment/Documents/annex/MEPC%2080/Annex%2015.pdf

Industrial Cybersecurity Pulse. (2021). Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

International Maritime Organization. (2014). SOLAS XI-2 and the ISPS Code. Retrieved in 2023, from IMO: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Jones, S. (2015). Addressing cyber security risks at ports and terminals. Port Technology International Journal, 62.

Official Journal of the European Union. (2016). Paris Agreement. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1019(01)

Official Journal of the European Union. (2021). European Climate Law. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1119

Rødseth, K. L., Schøyen, H., & Wangsness, P. B. (2020). Decomposing growth in Norwegian seaport container throughput and associated air pollution. Transportation Research Part D: Transport and Environment, 85, 102391. doi:https://doi.org/10.1016/j.trd.2020.102391

Spencer, T., Brooks, S. M., Evans, B. R., Tempest, J. A., & Möller, I. (2015). Southern North Sea storm surge event of 5 December 2013: Water levels, waves and coastal impacts. Earth-Science Reviews, 146, 120-145. doi:https://doi.org/10.1016/j.earscirev.2015.04.002

The European Scientific Advisory Board on Climate Change. (2023, 11 27). Climate Advisory Board. Preluat de pe https://climate-advisory-board.europa.eu/

The Institution of Engineering and Technology. (2020). Good Practice Guide - Cyber Security for Ports and Port Systems. United Kingdom. https://assets.publishing.service.gov.uk/media/5e284eefe5274a6c3ee68fcd/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Tran, N. K., & Haasis, H.-D. (2015). An empirical study of fleet expansion and growth of ship size in container liner shipping. Int. J. Prod. Econ, 241-253.

United Nations. (2015, 10 21). Resolution adopted by the General Assembly on 25 September 2015 Transforming our world: the 2030 Agenda for Sustainable. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/291/89/PDF/N1529189.pdf?OpenElement

United Nations Conference on Trade and Development. (2019). Review of Maritime Transport. https://unctad.org/system/files/official-document/rmt2019_en.pdf

Wild, P. (2021). Recommendations for a future global CO2-calculation standard for transport and logistics. Transportation Research Part D: Transport and Environment, 100, 103024. doi:https://doi.org/10.1016/j.trd.2021.103024

Zarzuelo, I. d. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. Transport Policy, 100, 1-4. doi.org/10.1016/j.tranpol.2020.10.001