GIS Odyssey Journal

2024 • Volume 4 • Number 1

https://doi.org/10.57599/gisoj.2024.4.1.131

Jakub Syta[1]

# CHALLENGES IN PROVIDING CYBERSECURITY TO PORT AND MARITIME INFRASTRUCTURE FACILITIES

**Abstract:** The following article focuses on the cybersecurity challenges within 'heavy' industries such as civilian ports and maritime infrastructure. Very often, such traditional sectors do not consider cybersecurity to be a priority. With the growing adaptation of modern technologies, the 5th generation of ports is approaching, where the exposition to cybersecurity threats will be huge. Additionally, the losses will not only be visible in 'cyberspace' but can cause significant infrastructure damage, injuries or even mass causalities. Or can impact the global supply chain. These threats are new, and often, port management never even had a chance to go through them. By discussing several real-life and imaginary examples, the author wants to highlight the reality of the impact of cybersecurity in-cidents. In his opinion, such examples should be widely distributed and shared not only with the CEO. The article ends with several recommendations to be implemented by port and maritime infrastructure executives.

**Keywords:** cybersecurity, cyberthreats, maritime industry, port infrastructure

Received: 26 July 2024; accepted: 1 October 2024



[1] Maritime Cybersecurity Center, Polish Naval Academy, Gdynia, Poland, ORCID ID: 0000-0002-0115-6432, email: j.syta@amw.gdynia.pl

## Introduction

For years, cybersecurity been associated mainly with actions of powerful states and their intelligence services, or threats dealt with only by the wealthiest banks. For this reason, many organisations operating in industries far from the latest technology, have not prioritised this issue.

However, the situation is different now. Any organisation can be affected any-time – not just those that conduct all their business in cyberspace. Cyberattacks also affect those whose activities are primarily visible in the 'real world', e.g. manufacturing companies, stockyards or maritime logistics. Such organisations often place their priorities elsewhere, claiming, not unreasonably, that the IT just supports their core processes. Too often they realise later, in a very painful way, that this 'supporting' area has grown, to become critical for ensuring the continuity of the entire organisation.

In this article, Author aims to present the diversity and relevance of cybersecurity issues for the wider port and maritime infrastructure based on historical and hypothetical examples. The issues are divided into fraud, various incidents ending in disrupting business processes, and upcoming threats, which are still rare but may play an increasingly important role over time.

## Methods

The following study is based on a literature review focusing on a real life and hypothetical cyberincident scenarios. Author created a synthesis of these scenarios and divided them into a proposed structure of into fraud, disrupting business processes and upcoming threats. Reverences to exact articles are provided. Article is aimed to highlight the importance of understanding cyberthreats and the main way to conduct the latter implementation of efficient control mechanisms.

Especially in the area of cybersecurity too often a trend is visible to add new. Conduct new research, implement new product, propose new attack vector. Such pressure leads to FOMO being one of the main reasons for burnout of cybersecurity (Williams, 2022; Gartner, 2023).

By this article Author proposes to conduct a step back. Instead of rushing for 'new' he proposes to rethink why cybersecurity matters in maritime industry, deliberate whether implemented safeguards and projects conducted truly bring value.

## Research problem

Port and maritime infrastructure can be divided into linear and nodal (point) elements (Tubielewicz, 2015). Looking at their scope, relevant for further consideration, linear infrastructure elements include, among other things, buoys and lighthouses. Port infrastructure on the other hand includes, among other things, commercial, fishing, marina and war ports. A seaport is a facility located between land and sea which is technically, organisationally, economically and legally prepared for various types of

land-sea and sea-land relations. Port infrastructure can be divided into (Tubielewicz, 2015):

- port access infrastructure including, among others, canals, locks, breakwaters, motorways, railways;
- intra-port infrastructure, including quays, channels, basins, port roads, in-land waterway facilities and equipment, installation systems, and information circulation systems;
- port superstructure, including warehouses, yards, handling facilities, mechanised equipment, ancillary facilities and equipment.

Activities within these processes are deeply supported by the IT infrastructure, that ensures:

- Development of multi-modal transportation;
- Increasing the competitiveness of the port;
- More efficient use of infrastructure;
- Streamlining administrative and customs procedures;
- Facilitated cooperation in the maritime industry;
- Reduction of service time;
- Reducing the cost of maritime operations;
- Ability to handle more contractors at the same time.

Apart from the typical – generic support of IT systems aimed to facilitate business functions as finance, HR, administration & reporting there are dedicated systems typical to marine needs as for example SAR, e-Customs, oil-pollution control, shipping safety exchange systems, radar surveillance system. Additionally, as port infrastructure is usually highly automated a number of Operations Technology systems is present. Their support physical security, fire prevention and of course cargo management. What is important IT systems used in ports interact with a wide variety of organizations. An increasing amount of information is exchanged automatically within the following categories (Williams, 2022):

- mandatory declarations and manifests submitted to port authorities and national and international institutions;
- authorisation documents confirming, for example, permission to enter the port or unload;
- operational data related to the processes carried out by the port, e.g. refuel-ling needs or cargo operation schedules;
- financial data such as invoices and payments;
- navigation data (GPS, AIS).

These examples are relevant to further considerations in the provision of cybersecurity, because they highlight the variety of facilities that process (store, transmit, modify) information. Additionally – the basic properties of information security will be of entirely different importance for the different types of information processed in different facilities. The international standard ISO 27001 (ISO/IEC, 2023) as well as NIS2 directive (NIS2, 2022), establishing requirements for information security, indicates crucial role of information security properties:

- confidentiality – designed to ensure that information can only be communicated to authorised persons/processes;
- availability – confirming that the information can be used immediately when needed;
- integrity – ensuring that information has not been unauthorisedly modified and is consistent with each other;
- authenticity – which seeks to ensure that the information has not been faked and that it comes from the correct source.

All the above highlights the complexity of cybersecurity.

With the rapid expansion of global trade, a rapid increase in modernisation of maritime infrastructure can be observed in recent decades. In order to keep up with the needs of international trade, further modern technologies are being implemented. These include solutions for collecting and processing even faster the vast amounts of information, which are used, among other things, to automate operations. This is also linked to the definition and construction of the next generation of ports (Kaliszewski, 2017). The fourth generation of ports covered such topics as the quality of port services, IT usage, the development of a stakeholder environment or the existence of a port/sea cluster, the containerisation of cargo flows, usage of advanced automation solutions, full integration with the transport and forwarding industry, as well as TQM (Total Quality Management). The emerging 5th generation of ports is additionally expected to focus on customers and the local community, offering deep IT integration with stakeholders. For this reason, among others, the concept of Industry 4.0 is increasingly being implemented, which includes (Rüßmann et al., 2015):

- autonomous systems and robots;
- horizontal and vertical integration of used systems;
- use of cloud computing;
- 3D printing;
- processing of massive collections of information (Big Data);
- augmented reality;
- simulation management;
- ensuring cybersecurity.

Author would like to draw particular attention to the last of these points, as modern technology should only be implemented with adequate safeguards. Its importance is increasingly being signalled. Among the top three challenges for ports, cybersecurity is listed next to piracy and terrorism (Deep Trekker, 2020). The literature emphasises that the following attributes are crucial to the functioning of a port (Drougkas et al., 2019):

- speed and efficiency of operations;
- the ability to carry out activities in a safe manner;
- ensuring health and safety rules for staff;
- ensuring the integrity of the physical infrastructure.

Given that the above relies heavily on adequately functioning IT systems, ensuring cybersecurity is becoming one of the priorities for modern ports. In order to achieve this, it is necessary to identify and understand the threats that need to be protected

against in the first place. This is also one of the main tasks given to ports and other operators of crucial services by the NIS2 directive stating cybersecurity objectives around whole EU. National laws regarding the management of critical infrastructure also highlight that ports need to manage all their risks accordingly to threats.

## Discussion

Autor, basing on the literature review, created a synthesis of cybersecurity challenges that needs to be properly addressed by port authorities. These include observations within such areas as fraud, business process disruption and emerging threats. He states that cyberattacks on marine infrastructure are inevitable and have a potential to significantly harm world supply chain.

### Fraud

Fraud seems to be the most common type of attacks, as it is by far the easiest to carry out. Although many organizations, particularly those operating in the logistics industry, have been dealing with it for centuries, recent years have seen a great variety of new techniques used by criminals.

The most common attacks involve attempts to steal funds. So-called phishing attacks aim to deceive recipients, convincing them to perform potentially dangerous actions, such as opening an e-mail attachment, passing credentials on a fraudulent website or revealing sensitive data. The more straightforward attacks require further interaction with the victim – to run scripts or install additional software. It is essential nowadays to use advanced security systems and to teach employees to recognize fraudulent messages. This is done through so-called social engineering tests and awareness training.

Once a malicious code has been installed on a victim's computer, the criminal can learn the victim's credentials, such as logins and passwords to their (often online) business tools. They can then attempt to:

- modify static data, e.g. account numbers held in databases or spreadsheets, while waiting for the victim to start sending him or her data themselves;
- modify money transfers in the course of their execution (the so-called man-in-the-middle technique), which is more complicated but also feasible, e.g. by modifying ac-count numbers as they are pasted from memory into banking systems;
- redirect the victim to the website of a fake bank, hoping that the victim will indicate as ‘trusted’ an account controlled by the criminals without reading the messages from the banking application;
- start further correspondence on behalf of the victim in an attempt to deceive other people – e.g. to convince them to send a transfer to a fictitious account or to in-stall malicious software.

The latter example is often used for attacks such as Business E-mail Compromise (BEC). The fraudsters impersonate an ‘important person’ – e.g. an executive of a company or a representative of a counterparty known to the victim from other –

genuine – transactions. An appropriate, plausible story is then created, and time pressure is exerted in the expectation that the victim will 'exceptionally' not follow all the 'bureaucratic' procedures and 'smoothly' fulfil the request. For example, in this way criminals attempt to change existing account numbers, successfully stealing multimillion-dollar sums (Roberts, 2017; TVN24, 2013).

It is worth noting that the scams described above do not necessarily have to in-volve attempts to steal funds. Looking at attacks that could particularly harm organizations operating in the port and logistics industry, attack scenarios can be much 'more interesting', for example, they may involve attempts to:

- release of goods to an unauthorized person;
- modify information related to content to facilitate smuggling or sanction avoidance;
- redirect the container to another location in order to harm competition or support its latter disappearance;
- hide containers used for criminal activities, e.g. drug smuggling (Ubmemea, 2013), human trafficking or even use as torture chambers (The Telegraph, 2022);
- provide extract information on the detailed content of the containers to support latter theft.

From authority perspective a 'simple' money loss might seem less devastating than any of the above examples. The above examples are intended to illustrate how important it is for the operation of ports and related organizations to straighten their internal control processes to ensure the confidentiality, integrity, authenticity and ac-countability of information.

**Disruption of business processes**

The malware infection, mentioned in the previous chapter, has also other effects, more visible than the theft of credentials. When criminals realize, they have managed to get into an organization's internal network handling a significant amount of money, they increasingly resort to blackmail. Instead of stealing hundreds of thousands or few millions of dollars – a typical BEC scam – they prefer to receive a much more enormous ransom by attacking another information security property – its availability. At the time of writing this article, the largest, known to Author, ransom demanded by criminals was $50,000,000 (Abrams, 2021).

This is achieved using what is known as a ransomware attack. It involves encrypting servers and workstations containing business-critical data. It might focus on business systems with cargo information of production systems or steering and maneuvering. Very often, at the same time, criminals are able to encrypt backups. As computers control the infrastructure, process information about goods, routes, senders, and recipients, the loss of this information leads to massive problems not only among companies operating directly in the logistics industry. It touches all areas of the economy, as was possible to notice during successful attacks on logistics companies such as Maersk (Chirgwin, 2018) (which had to spend around $300 million to restore operations after the cyberattack), COSCO and MSC (Kapadia, 2020), as well as port

operators such as Barcelona (Esage, 2018) or San Diego (Tsonchew, 2018). The inability to receive components stops production processes in factories, unclaimed goods spoil while waiting for too long. Understandably, in such situations multi-million-dollar legal demands are set against those guilty of negligence in IT security.

Restoring all IT systems is a task of days or even weeks, depending on the size of the IT infrastructure. Above all, it requires having the most up-to-date backups possible, which needs to be addressed. However, the part of companies that do have up-to-date backups and want to restore business continuity themselves face another threat. In order to further force companies to pay the ransom, criminals first steal sensitive data and threaten to publish it. Organizations have been known to decide to pay the ransom in such situations. It is worth noting here that it is not certain that criminals will hand over decryption codes after obtaining the ransom. Nor is it evident that the codes handed over will definitely work. And even if they do, it is essential to remember that it can take weeks to recover the encrypted infrastructure. One 'variant' or ransomware attacks is called a wiper. It also encrypts data or makes them unavailable in different ways, but there is no way to recover them. This is a typical devastating at-tack.

Another type of attack that can decisively hamper customer communication are DDoS attacks. Although less noticeable than in previous years, they constantly in-crease in volume. At the time of writing, the unofficial world record holder was an at-tack with a volume above 398 000 000 requests per second and by a botnet od 20 000 compromised machines (Powell, 2023). Such powerful attacks, if not stopped by advanced security systems, are capable not only to block customer related traffic for the entire duration of the attack but also can disable network devices, preventing access to the infrastructure for the duration of the repair. This could be especially dangerous for business in-formation exchange systems.

However, these are not only 'typical' internet attacks that are capable of blocking functioning of a port. Collisions caused by unauthorized manipulation of communication means, described in the next chapter, or a cyber-supported sabotage could potentially lead to blocking routes (Christian, 2021) or port infrastructure. And there are an increasing number of cases of malware infecting maritime infrastructure (Knit 360, 2021). It remains a question of time when successful attacks will harm the work of locks or breakwaters. Extremely interesting attacks on locomotives (BadCyber, 2023) or rail systems (Roth, 2022), that can be sometimes considered as a part of port superstructure, already took place.

**Emerging threats**

The issues described earlier in this article are already a daily occurrence. Phishing campaigns, BEC fraud, ransomware or DDoS attacks affect dozens or even hundreds of entities every day – including port operators or logistics companies – one can read about new cases in different industries on a daily basis. This article section will highlight emerging cyberthreats specific to port and maritime infrastructure. Even though they are not necessarily completely new, in Authors opinion one could expect their significant rise of occurrence and even more devastating consequences.

Most ships use a GPS signal for navigation. However, this technology is not immune to attacks, and there are possibilities of jamming or spoofing the signal. This has been observed, for example, during military maneuvers (Goward, 2018), although not in all cases clear correlations are apparent (The Navigation Center of Excellence, 2024). These attacks are not new, but more and more often they last for many days and cover large areas (Kiev Post, 2024). Attempts to impede the navy's exercises or operational activities can also affect civilian units. Also a number of AIS attacks raised (Euromaidan Press, 2023) – signals can be blocked, faked – sometimes even the work of whole AIS stations is interrupted. Such actions can lead, for example, to collisions or running aground and consequent loss of part of the cargo, damage to the vessel and even environmental disasters. GPS and AIS attacks became very common, especially from the moment Russia invaded Ukraine. Still another potential target one needs to be aware of are buoys (Mu et al., 2020) and lighthouses that can lead to collisions.

Yet another threat that would primarily manifest in ports would be jamming RF communications between harbors and ships. Radio communications are often not immune to attempted attacks, and jamming a radio channel could, at best, lead to confusion and, in worse scenarios, to collisions. To make matters worse, carrying out this type of attack does not require a significant financial outlay. However, some protection is provided by the need to get physically close to the infrastructure under attack.

Ultimately, new risks will emerge with the proliferation of autonomous ships. Work in this area has been going on for years. It is so advanced that it is already primarily due to regulatory considerations that they are not something that can be observed on a daily basis. However, autonomous vessels are susceptible to communication interference, which is not difficult to occur at sea. Decisions are made based on machine learning algorithms, which are also sometimes susceptible to manipulation and deception, resulting in irrational decisions (OpenAI, 2021; Nassi et al., 2020). Sophisticated attacks on autonomous vehicles, such as AGVs, can also create chaos and lead to accidents, contributing to the disruption of business processe (Kemme, 2013). Especially when one takes into account that unexpected ‘easter eggs’ can already be hidden inside the source code of transport machines (BadCyber, 2023). And that cyberattacks targeted ships already are known (Dark Reading Staff, 2024). Although the mentioned hack most probably focused on intelligence-gathering systems on a ship, it demonstrated that ships were recognized as potentially very interesting targets.

Industry 4.0 stipulates the usage of robots and autonomous systems. Usage of robots in port work, despite their obvious benefits, can again lead to tragedy (DW, 2015), especially if criminals will be able to influence their operation in an unauthorized way. Author hopes that the number of fatalities will remain low, but at the same time expects that the number of interruptions, accidents, failures or errors will increase with the proliferation of IIoT (Industrial Internet of Things) devices. Indeed, it should be emphasized that IIoT devices commonly used as sensors and controllers are very often prepared against the best cybersecurity practices (IoT Security Foundation, 2024). Low cost IIoT usually leads to unsecure devices.

## Recommendations

Examples of historical as well as hypothetical cyberattacks could be multiplied. However, this is not the purpose of this article. What is important is ensuring that decision-makers will be able to make aware decisions about the implementation of new technologies – taking into account both apparent benefits and less obvious risks. Providers of new technologies should be required to prove due care while reducing the likelihood of various types of cyberincidents or ensure that their potential impact is decisively reduced. However, there is no way to achieve this when price is a crucial, or sometimes the only factor while technology selection. Risk analysis should be mandatory for the implementation of new technologies. In extreme cases cyberrisks can lead to losses that exceed the value of the investment. And even more – cyberattacks target-ed at industry environment often might result in so called '3D': Deny, Degrade and Destroy. This from local perspective might cause injuries or fatalities and from larger perspective might delay or stop supply chain. Proposals for the most effective controls and extensive risk catalogues are already widely available (Drougkas et al., 2019).

Although Author is a strong advocate of the use of modern digital technologies, he suggests to maintain the ability to sustain the continuity of key business processes in the traditional – manual/analogue way. As demonstrated in the previous chapters, the rush to digitalisation and the introduction of the 'Internet of Everything' model (Langley et al., 2021), are full of threats. Above all, those related to the deliberate, harmful activities of criminals, but also caused by the level of complexity. Although this type of operation is much slower and cannot guarantee productivity levels, safety considerations should lead to the fact that at least some of the most critical processes can be sustained in this way.

A good starting point for securing the infrastructure would be – for each of the major seaports – to conduct a cybersecurity review and identify standardised control mechanisms that would bring risk to a level acceptable to port authorities and key stakeholders.

Such a cybersecurity review serves as an excellent basis to perform further – more constructive activities. The author is a huge advocate of following industry standards. Their value very often covers complex approaches to a subject. The author very often worked on projects that aimed to protect small areas that did not impact the organisation's cybersecurity posture and did not focus on creating value. IT especially was true in Operations Technology (OT) cybersecurity projects. To protect this area, which is extremely important in the maritime industry, it is crucial to understand that the topic is too complex to be managed within one project. OT cybersecurity can be managed from the perspective of:

- secure IoT, IIoT and similar devices that should be selected with cybersecurity requirements in mind;

- secure OT architecture, that should be separated from the Internet if only possible, to prevent cyberattacks from causing damages in the 'real world' – also resulting in explosions and other causalities;
- security management system that will cover secure components, pre-pared in line with secure processes, that are processed using secure technologies.

Some other best practice control mechanisms, looking from the perspective of identifies types of attacks and given examples are mentioned bellow. It is important to highlight that these are not complete catalogues and that they might repeat themselves.

**Fraud**

- constant, managed awareness training that includes social-engineering tests;
- anti-phishing mail and instant management filtering system;
- Cyber Threat Information system subscription listing fraudulent sites that will be automatically blocked on DNS level;
- Hardened business processes;
- Dual control while performing risky tasks as the modification of static data (e.g. bank account numbers of main business partners);
- Rapid incident reporting procedures;
- Endpoint Detection and Response (EDR) systems;
- Vulnerability management;
- Penetration tests with follow-up activities;
- Cyber-insurance.

**Disruption of business processes**

- Endpoint Detection and Response (EDR) systems
- Vulnerability management;
- Penetration tests with follow-up activities;
- Tested backups;
- Separated infrastructure for IT and OT systems;
- Data Leakage Protection systems;
- Anti-DDoS Systems;
- Business Continuity Plans and Disaster Recovery Plans;
- Cyber-insurance.

**Emerging threats**

- Business Continuity Plans and Disaster Recovery Plans;
- Backup communication;
- Endpoint Detection and Response (EDR) systems;
- Network Detection and Response (NDR) systems;
- Security Orchestration, Automation and Response (SOAR) systems added to Security Incident & Event Management (SIEM) systems ;
- SOC and CERT teams and established cooperation with respective CSIRT teams;
- Separated infrastructure for IT and OT systems;
- Cyber-insurance.

These are just the examples, and the exact decision ought to be taken basing on the results from the risk evaluation including the financial, reputational and regulatory impact of cyberincidents.

## Conclusions

Modern digital solutions in ports are helping to reduce container unit handling times and increase terminal throughput (Kuźmicz et al., 2020). Increasing automation of container terminals will allow it to handle the increasing number of cargoes handled. The deployment of autonomous vehicles and equipment will increase productivity and reduce costs in many areas. On the other hand, platform-equipped vehicles will enable the container to be loaded autonomously without the help of additional equipment, which will affect a faster loading and unloading process. The deployment of Unmanned Aerial Vehicles for efficient inspection of hard-to-reach equipment (such as cranes and overhead cranes) will increase the efficiency of the terminal's operations. Many analyses show how to develop ports' operations, but among the threats, one can rarely find a reference to the necessity of adequate (cyber)security.

Sources indicate that one of the significant challenges to address will be the approach of port authorities to security, as the introduction of solutions beyond those defined just as baseline requirement (Zawadzki, 2019; NIK, 2018). Consequently, security has always been a lower priority than fundamental infrastructure investments. However, a slow change in trends can be seen, and it can be expected that in the future, shipowners will be more and more willing to choose ports where their vessels and cargo will be secure.

Manufacturers of security systems are offering more and more modern solutions. However, even the best systems will not fulfil their role if they do not function in adequately designed structures based on well-formalised rules. Maritime infrastructure authorities need to be aware of possible consequences. For many years heavy industry was not a target for cybercriminals. It changed. But it will not only be ports to face consequences – such cyberattacks could have impact on the whole society. Cyberattacks on marine infrastructure are inevitable and have a potential to significantly harm world supply chain. Early and comprehensive building of staff awareness of cybersecurity is through a must (Canepa et al., 2021). Understanding the possible consequences of various cyberattacks can lead to better business decisions.

## Acknowledgements

This article is a part of statutory activities performed by Maritime Cybersecurity Center at Polish Naval Academy.

## References

Abrams L. (2021). Computer giant Acer hit by $50 million ransomware attack. https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/ [access: 01.06.2024].

BadCyber (2023). Dieselgate, but for trains – some heavyweight hardware hacking. https://badcyber.com/dieselgate-but-for-trains-some-heavyweight-hardware-hacking/ [access: 01.06.2024].

Canepa M., Ballini F., Dalaklis D. Vakili S. (2021). Assessing the effectiveness of cybersecurity training and rising awareness within the maritime domain. 10.21125/inted.2021.0726. 2021.

Chirgwin R. (2018). IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz. https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/ [access: 01.06.2024].

Christian A. (2021). The untold story of the big boat that broke the world. https://www.wired.co.uk/article/ever-given-global-supply-chain [access: 01.06.2024].

Dark Reading Staff (2024). Iran Warship Aiding Houthi Pirates Hacked by US. https://www.darkreading.com/cyberattacks-data-breaches/iranian-ship-aiding-houthi [access: 01.06.2024].

Deep Trekker (2020). Top 3 Risks at our Ports. https://www.deeptrekker.com/resources/maritime-port-security-risks [access: 01.06.2024].

Drougkas A., Sarri S., Kyranoudi P., Zisi A. (2019). Good practices for cybersecurity in the maritime sector, ENISA 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector [access: 01.06.2024].

DW (2015). Robot kills worker at Volkswagen plant in Germany. https://www.dw.com/en/robot-kills-worker-at-volkswagen-plant-in-germany/a-18556982 [access: 01.06.2024].

Esage A. (2018). Hacking attack in port of Barcelona. https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/ [access: 01.06.2024].

Euromaidan Press (2023). Maritime security in the Black Sea is an international problem. https://channel16.dryadglobal.com/maritime-security-in-the-black-sea-is-an-international-problem [access: 01.06.2024].

Gartner (2023). Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024. https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024 [access: 01.06.2024].

Goward D. (2018). GPS disrupted for maritime in Mediterranean, Red Sea. https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/ [access: 01.06.2024].

IoT Security Foundation (2024). https://www.iotsecurityfoundation.org/ [access: 01.06.2024].

ISO/IEC (2023), ISO/IEC 27001:2023 Information technology – Security techniques – Information security management systems – Requirements, ISO 2023.

Kaliszewski A. (2017). Fifth and sixth generation ports (5GP, 6GP) – the evolution of the economic and social role of ports, Studies and Materials of the Institute of Transport and Maritime Trade.

Kapadia S. (2020). 3 years, 3 cyberattacks on major ocean carriers. How can shippers protect themselves? https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/ [access: 01.06.2024].

Kemme, N. (2013). Design and Operation of Automated Container Storage Systems, Physica-Verlag Heidelberg.

Kiev Post (2024). Recent GPS Failures in Poland and Baltic States Blamed on Russian Electronic Warfare Trials. https://www.kyivpost.com/post/26945 [access: 01.06.2024].

Knit 360 (2021). Collaboration in the Shipping Industry: Innovation and Technology https://knect365.com/maritime/article/91705d00-6d9d-4ba3-98a4-9b10c92ad520/epaper-collaboration-in-the-shipping-industry-innovation-and-technology [access: 01.06.2024].

Kuźmicz K., Glinko M., Kondraciuk S., Kowalczuk Ł. (2020). Analysis of the automation potential of the container terminal in Gdansk. Academy of Management 4(3), Faculty of Management Engineering, Bialystok University of Technology 2020.

Langley D., van Doorn J., Ng I. Stieglitz S., Lazovik A., Boonstra A. (2021). The Internet of Everything: Smart things and their impact on business models. Journal of Business Research, vol. 122.

Mu L., Zhao E., Wang Y., Zomaya A. (2020). Buoy Sensor Cyberattack Detection in Offshore Petroleum Cyber-Physical Systems. https://www.researchgate.net/publication/338440318_Buoy_Sensor_Cyberattack_Detection_in_Offshore_Petroleum_Cyber-Physical_Systems [access: 01.06.2024].

Nassi B., Nassi D., Ben-Netanel R., Mirsky Y., Drokin O., Elovici Y. (2020). Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems, Ben-Gurion University, Negev, Israel. https://eprint.iacr.org/2020/085.pdf [access: 01.06.2024].

NIK (2018). Information on the results of the audit, Seaport Access Infrastructure, KIN.430.003.2017 Record No. 37/2018/P/17/033/KIN. https://www.nik.gov.pl/plik/id,17942,vp,20530.pdf [access: 01.06.2024].

NIS (2022). EU Directive on Security of Network and Information Systems (NIS2 Directive) – proposal for a new directive available at https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union [access: 01.06.2024].

NIS2 (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

OpenAI (2021). Multimodal Neurons in Artificial Neural Networks. https://openai.com/blog/multimodal-neurons/ [access: 01.06.2024].

Powell O. (2023). Largest DDoS attacks ever reported by Google, Cloudflare and AWS. https://www.cshub.com/attacks/news/record-breaking-ddos-attack [access: 01.06.2024].

Roberts J. (2017). Exclusive: Facebook and Google Were Victims of $100M Payment Scam. https://fortune.com/2017/04/27/facebook-google-rimasauskas/ [access: 01.06.2024].

Roth A. (2022). Cyberpartisans' hack Belarusian railway to disrupt Russian buildup, https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup [access: 01.06.2024].

Rüßmann M., Lozenz M., Gerbert P., Waldner M., Engel P., Harnish M. (2015). Industry 4.0: the Future of Productivity and Growth in Manufacturing Industries. Technical Report. Boston Consulting Group. https://image-src.bcg.com/Images/Industry_40_Future_of_Productivity_April_2015_tcm9-61694.pdf [access: 01.06.2024].

The Navigation Center of Excellence (2024). GPS Problem Reports Status https://navcen.uscg.gov/?Do=GPSReportStatus. [access: 01.06.2024].

The Telegraph (2022). Inside the Dutch 'torture chamber'. https://www.telegraph.co.uk/news/2022/04/02/inside-dutch-torture-chamber/ [access: 01.06.2024].

Tsonchew A. (2018). Troubled waters: cyber-attacks on San Diego and Barcelona's ports. https://www.darktrace.com/en/blog/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports/ [access: 01.06.2024].

Tubielewicz A. (2015). Logistical management in maritime transport. Oficyna Wydawnicza Polskie Towarzystwa Zarządzania Produkcją, Gdańsk.

TVN24 (2013). Zapłacili oszustowi. Lecą głowy w Metrze Warszawskim (*They paid the scammer. Heads are flying in the Warsaw Metro*). https://tvn24.pl/tvnwarszawa/najnowsze/zaplacili-oszustowi-leca-glowy-w-metrze-warszawskim-241057 [access: 01.06.2024].

Ubmemea (2013). Antwerp incident highlights maritime IT security risk. https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk [access: 01.06.2024].

Williams D. (2022). Nearly a Third of Cybersecurity Leaders Considering Quitting. https://www.blackfog.com/cybersecurity-leaders-consider-quitting/ [access: 01.06.2024].

Zawadzki J. (2019). Integrated port security post factoring in the optimal use of the potential of security forces and measures. Maritime Security Yearbook, Polish Naval Academy.