CYBER THREATS TO MARITIME CRITICAL INFRASTRUCTURE

Andrej Androjna, Elen Twrdy

(University of Ljubljana, Faculty of Maritime Studies and Transport, Portorož)

Keywords: cyber security, cyber threats, maritime critical infrastructure, jamming.

ABSTRACT:

The increasing speed of the development of information and communication technologies (ICT) and the constant connection to the internet bring new cyber threats, thus increasing the chances of cyber-attacks targeting maritime critical infrastructure. In terms of improving the efficiency of port operations, their vulnerability (e.g. consequences in the event of a system failure) is increasing with the interconnection and integration of many maritime and logistics systems. The impact of the tools available to attackers for cyber-attacks are not yet fully understood. This is precisely why the protection, or cyber security, of maritime critical infrastructure is becoming one of the major issues of national security and economic stability. Port security and the efficiency of port operations are crucial not only for maritime transport but also for their strategic role in terms of security at the national, regional and European level. This article presents new challenges, threats and strategies in overcoming barriers in the context of ensuring the cyber security of maritime critical infrastructure.

1. INTRODUCTION

1.1. Definition of maritime critical infrastructure in the Republic of Slovenia

The critical infrastructure of national importance in the Republic of Slovenia encompasses those capacities that are crucial to the country. The suspension of its operation or its destruction would have a significant impact on national security, the economy, and other key social functions, as well as on the health, safety, protection and wellbeing of the people.

The identification and designation of critical infrastructure, the principles and planning of its protection, the tasks of bodies and organizations in the field of critical infrastructure, and the communication, reporting, decision-making support, data protection and control in the field of

critical infrastructure are governed by the *Critical Infrastructure Act* (2017). The law defines the following sectors as critical infrastructure: energy, transport, food, drinking water, healthcare, finances, environmental protection, information and communication networks and systems.

Maritime critical infrastructure is defined as a capacity whose serious malfunction or activity interruption could impede port operations in the Port of Koper for at least a week. The Port of Koper d.d. represents a great generator of development in Slovenia, so its smooth and safe operation is crucial. Any serious malfunction of the operations in the Port of Koper d.d. would affect the interruption of goods flows away from and into Slovenia. Therefore, great care should be taken to ensure the safety of this critical infrastructure.

1.2. European Critical Infrastructure

The European Critical Infrastructure (ECI) of the Republic of Slovenia is the infrastructure located within the territory of our country, and is determined in accordance with the regulations governing European Critical Infrastructure. The ECI in the Republic of Slovenia is regulated by the *Regulation on European Critical Infrastructure* (2011) which transposes into the acquis of the Republic of Slovenia in the *Directive on the Identification and Designation of European Critical Infrastructures and Assessment of the Need to Improve their Protection*.

The European Union has identified ports as critical infrastructure; the term "port" means any designated land and sea area with boundaries defined by the Member State in which the port is located, and equipment and infrastructure to facilitate commercial maritime transport (Directive 2005/65/ES3).

In fact, ports are today the key intermodal hubs in both the freight and passenger transport networks of the European Union (EU). In addition to being important border checkpoints, they also play an important role in international trade. Maritime goods flows are constantly expanding, and maritime transport confirms its crucial role in the functioning of our society and our economy (SECNET, 2019).

The security of ports and the efficiency of their operations is therefore crucial not only for maritime transport, but also for their strategic role in terms of security at the regional, national and European levels. Port security is thus an opportunity to automate and simplify procedures and activities in ports (Andritsos, 2013), and can also benefit from information and communication technology (ICT).

In the context of physical and cyber security, new challenges, threats and strategies to overcome them have led to ports' automation and digital transformation, the optimization of existing processes, the monitoring of real-time operations, the interconnection of information technology (IT) and operational technology (OT), and the deployment of new technological capabilities (e.g. cloud computing, the Internet of Things (IoT), etc.).

2. PORT INFRASTRUCTURE

Port infrastructure and services are quite diverse across EU Member States. Over time, ports have adapted their infrastructure and services to local geographical features and activities related to their location (fishing pools, tourism, etc.) and the various challenges they have had to face. Port infrastructure ensures that vessels can be safely anchored and moored, allows vessels to pass between water areas at different levels (e.g. barriers), or provides facilities for the construction and repair of vessels (e.g. dry docks). It consists of marine (waveguides, excavation, barriers, river basins, coast, piers, moorings, etc.) and land infrastructure (inland roads, railways, promenades, etc.), administration buildings, and terminals. The management of port facilities is usually entrusted to private terminal operators who are in charge of managing and maintaining the upgrades (such as transhipment machinery, silos, special fences, control devices, passenger terminals) to carry out individual operations or activities related to the transhipment of maritime goods (shipping containers, general cargo, bulk cargo, petroleum products, etc.), passengers or motor vehicles (Ro-Ro and passenger ships), and fisheries (transhipment, inspection, etc.).

The fact is, however, that new technologies are, in principle, changing all maritime activities from navigation to freight transport management, e.g. customs clearance, setting deadlines, delivery, storage in warehouses, storage on board ship, and the management of all communications and information about the movement of goods and people to which large quantities of money-related data are connected and which are susceptible to cyber-attacks (ENISA, 2019).

2.1. Port connections to the hinterland

Transport connections with the hinterland are a prerequisite for the existence and development of a port. They affect the operation of each port, since without proper connections no port could provide the necessary services to its hinterland.

No special technology is required to connect ports to road transport; only truck access to the storage areas where cargo is transhipped is required. This means that in addition to the roads, a

large enough parking space is needed where trucks can wait and complete all the necessary customs formalities. The entry and exit of trucks to and from a port presents a particular problem. Everybody must carry out the entry and exit procedures at a certain place, which causes congestion and therefore heavy traffic.

However, the connection of a port to the railway network does require special infrastructure. It is important that the piers where the goods are transhipped are equipped with rails, since the operation time is significantly shorter. The optimal and direct connection of a port railway infrastructure to the main railway infrastructure in an individual country is essential here, as the aim is to transport as much cargo as possible to the hinterland by train.

The technical equipment of a port and good organization of work are very important because the quality of service and the success of the port depend on this. It is therefore necessary to constantly adapt to the rapid development of transport technologies and new technological requirements such as digitization and automation. This is especially true for those port operations which are today dependent on information technology.

2.2. Port operations

Roberts (2015) states that today cargo handling is the focus of port operations, but its tracking system is not the only one that is exposed to cyber threats. Today, ports rely as much on computer networks as they do on stevedores. Special network control systems control the loading and unloading of cargo. All types of transhipping equipment, such as container manipulators and portal transporters, now use technologies such as optical recognition of port operations management, including cargo localization, transportation, inspection, and so on. In state-of-the-art ports (Rotterdam), shipping containers are automatically loaded/unloaded and moved using GPS (Kramek, 2013). Vehicles that automatically transport cargo from terminals are also highly dependent on the efficient operation of GPS, which makes the modern port operating system vulnerable. Potential GPS jammers can make it difficult or even impossible for an entire port to operate. The closure of a port may result in a revenue loss of several million (including a consequent impact on GDP at both regional and national levels) (Orsoz, 2010; Business Wire, 2015).

3. REGULATION AT INTERNATIONAL AND EUROPEAN LEVELS

The EU does not only have interests but also duties in global maritime security. It therefore actively contributes to safety and security at sea in different parts of the world, making use of several existing EU instruments such as the Instrument contributing to Stability and Peace (IcSP) and the European Development Fund, as well as EU policies such as the Common Security and Defence Policy (CSDP).

3.1. Regulation at international level

At the international level, the SOLAS Annex XI-2 was added in 2002 to the *International Convention for the Safety of Life at Sea – SOLAS* (IMO, 1974), resulting in the *International Ship and Port Facility Security – ISPS* (IMO, 2002), which introduces, in particular, measures aimed at enhancing the protection of merchant ships in international and inland liner shipping, as well as port security measures (including cyber security). The Code obliges Member States to prepare *Port Facility Security Assessments* (PFSA) for all their ports, which should take into account the specificities of the different port units (physical security, integrity structure, personnel protection systems, procedural policies, radio and telecommunications systems, computer systems and networks, and transport infrastructure), as well as containing a *Port Facility Security Plan* (PFSP) within the port boundaries (access, restricted areas, cargo handling, delivery of shipping, and security controls).

The *Convention on Facilitation of International Maritime Traffic* (FAL) by the International Maritime Organization (IMO 2017) simplifies and harmonizes the procedures of maritime transport by standardizing the use of electronic information transmission (the "Single Window" concept – SafeSeaNet), and streamlining reporting formalities for ships in the process of sailing in and out of the port.

Cyber security in international maritime space is only specifically tackled by the *Guidelines on Maritime Cyber Risk Management* (IMO, 2017) which aim to raise awareness of the protection and enhancement of the flexibility of cyber systems supporting the operation of ports, vessels, maritime facilities and other elements of the maritime transport system (IT, OT).

3.2. Regulation at the level of the European Union

Legal acts and decisions concerning maritime safety improvement measures taken in an international environment are directly or indirectly related to EU law:

- Certain chapters of the SOLAS Convention have been transposed into the EU by several regulations: *Regulation (EC) 725/2004* relates to the enhancement of ship and port facility

security and the implementation of the International Ship and Port Facility Security Code (ISPS), while *Directive 2005/65/EC* focuses on enhancing port security. *Regulation (EC) 336/2006* governs the implementation of the *International Safety Management Code within the Community – ISM* (IMO, 1995/2017) in the maritime sector of the Community, but does not apply to ports;

- *Directive 2010/65/EU* defines the formalities (FAL forms) of reporting ships arriving in and/or departing from ports of the Member States and dictates the introduction of the *SafeSeaNet* system for the secure exchange of information between Member States' maritime authorities and other authorities (e.g. customs systems).

In 2014, in support of the protection of the interests of the EU and the protection of its Member States and citizens, the EU adopted the *European Union Maritime Security Strategy* (EUMSS, 2014) and its Action Plan, which combines the internal and external aspects of EU maritime security. It tackles maritime risks and threats on a global scale, including cross-border and organized crime, threats to freedom of navigation, critical maritime and energy infrastructure, cyber security, threats to biodiversity, illegal, unreported and unregulated fishing, and environmental degradation through illegal or unintentional releases.

With the increasing digitalization of business and the rapid development of information and communications technology, the volume of personal data collection and the flow of information about users is increasing. This creates more and more opportunities for abuse and violation of privacy rights. For this reason the EU adopted the *General Data Protection Regulation – GDPR* (2016) which aims to harmonize and raise the level of protection of personal data in various sectors of the EU, including the maritime sector.

The European Union has developed a comprehensive cyber security policy to prevent and combat cybercrime. In May 2018, a new *Cybersecurity Act* came into force to strengthen Europe's cyber resilience. The European Union Agency for Cybersecurity (ENISA) was also set up to assist Member States in effectively preventing and responding to cyber-attacks.

In connection with cyber security at the EU level, *Directive 2016/1148* (NIS Directive) was adopted concerning measures for a high common level of security of network and information systems across the Union. The maritime sector is subject to the security requirements applicable to businesses, ships, port infrastructure, ports and shipping services, including radio and telecommunications systems, computer systems and networks. It was also defined that Member

States should take into account the existing and future international codes and guidelines, especially those developed by the IMO, in order to ensure a coherent approach for individual operators in the maritime sector when designating operators in the Water Transport Sector.
In addition to international and European legislative (including political) initiatives, several Member States have developed their own initiatives to improve cyber security at the national level and also with a focus on the maritime sector, such as national cyber security strategies, good practices or recommendations, for example, the French CIIP act, the British Code of Practice of Cyber Security for Ports and Port Systems, and the German "IT-Grundschutz," (ENISA, 2019).

4. EXAMPLES OF THREATS TO MARITIME INFRASTRUCTURE

According to the European Commission, the economic impact of cybercrime increased fivefold between 2013 and 2017 and could increase fourfold again by 2020. By 2016, 80% of European businesses suffered damage from attacks. Since the first known attack in Estonia in 2007, both citizens and entire countries have been affected (SECNET, 2019).

Today port authorities are, more than ever, facing increasing risks with ever-increasing responsiveness, so the area of their responsibility is constantly broadening.

4.1. *Infection of authentication data for high-value cargo theft or illicit trafficking in a targeted attack*

Among the more notable examples of an attack on port critical infrastructure is certainly the hacking attack in the Port of Antwerp in 2012, where computer hackers, in cooperation with drug cartels, invaded the computer system that monitors the movement of containers in the port and removed a shipping container before it had been controlled by the port authorities. The case, of course, was not isolated, but when the investigative authorities managed to identify the crime, the investigative action contributed to seizing a record eight tonnes of cocaine with a street retail price of EUR 500 million which had been hidden in a container full of bananas from Ecuador.

This attack was carried out using the method of social engineering and a malicious program sent via email. While in this particular case the intrusion was detected and certain countermeasures were applied by the port authorities, they were unable to contain another intrusion where specific hardware (mini-computers hidden inside distribution power cords and external computer data storage) and recording components mounted on a computer keyboard were used.

4.2. Infection of software leads to a complete shutdown of port operations

At the end of June 2017, the Petya virus, which spread through the internet, affected computers in more than 65 countries. The Ukrainian computer virus quickly disrupted various computer systems and did not spare even the largest companies such as the Danish shipwright Maersk, which was crippled by the virus for a few days. Maersk's downturn of several days caused damages of approximately $300 million. Although Petya was not a blackmail virus, it caused enormous damage as it was intended to erase data and disable the operation of various systems.

4.3. Infection of system software causes interference with port operations

System software designed to carry out port operations can be destroyed by a malware infection from the web which hacks into the most secured parts of computer memory, including its hardware, in the most cunning of ways. By taking full control of the system, it is possible to intercept all communications of its users over wired (Ethernet) and wireless networks (WiFi, UMTS, GPRS, Bluetooth etc.), and even carry out legally binding actions in their names, such as transfers of funds or entering into credit agreements through e-banking services or, last but not least, impeding port activities and even causing a work accident in the port.

5. CYBER SECURITY CHALLENGES

Based on various studies, it can be concluded that, in addition to physical damage insurance, the main challenges when trying to ensure the cyber security of ports are the following:

- Poor awareness and skills with regard to maritime information and cyber security,
- Lack of financial and other resources (e.g. cybersecurity experts) to ensure information security,
- The technical complexity of the port ecosystem,
- Finding the right balance between business efficiency and cyber security,
- The existence of outdated and vulnerable information systems,
- A lack of a regulatory framework for cybersecurity implementation,
- The interconnection of information technology (IT) and operational technology (OT),
- Security risks in the supply chain (lack of certificates, remote access of the supplier to the port, etc.),
- The heterogeneity of networks/systems,

- The involvement of all stakeholders in the provision of port cybersecurity,
- Cybersecurity does not keep pace with technological advances or developments and the emergence of new challenges related to the digital transformation of ports, etc.

6. CONCLUSION

We live in a time when the issue of security is an important part of our daily lives. The impact of the tools available to attackers for conducting cyber-attacks is not yet fully understood. This is why ensuring the protection or cybersecurity of maritime critical infrastructure is becoming one of the most important issues in national security and economic stability. Port security and the efficiency of their operations are crucial not only for maritime transport, but also for their strategic role in terms of security at the national, regional and European levels. This is especially true for Slovenia, which only has one maritime cargo port. The fact is that the operation and activities of ports are today becoming increasingly digitized and automated, and as a result more vulnerable to potential cyber threats. However, the consequences of the latter can be avoided or at least mitigated by adequately ensuring advanced security of the port infrastructure, establishing operational procedures, improving the resilience of computer networks/systems protection, increasing user awareness, and last but not least, considering security as part of the strategic management of a port.

REFERENCES:

- Andritsos, F. (2013). *EU port security & growth*. Proceedings of the 8th Future Security Research Conference, p 267-274 Fraunhofer. Retrieved March 02, 2020, from: http://publica.fraunhofer.de/ documents/*H-47052.html, ISBN: 978-3-8396-0604-9*
- Council of the EU (2018). *Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*. Brussels: Council of the EU.
- *Directive of the European Parliament and of the Council on enhancing port security* (2005). Directive of the European Parliament and of the Council, № 2005/65/EC of 26 October 2005.
- *Directive of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States of the Community* (2002). Directive of the European Parliament and of the Council, № 2002/6/EC of 18 February 2002.
- *Directive of the European Parliament and of the Council on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive*

2002/6/EC (2010). Directive of the European Parliament and of the Council, № 2010/65/EU of 20 October 2010.

- *Directive (EU) of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union* (2016). Directive of the European Parliament and of the Council, № 2016/1148 of 6 July 2016.
- *Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (2008). EU Council Directive № 2008/114/EC of 8 December 2008.
- *European Union Maritime Security Strategy* (2014). EU Council № 11205/4 of 24 Jun 2014.
- *GPS disruption halts ports, endangers ships – US Coast Guard*, Resilient Navigation and Timing Foundation. Retrieved February 10, 2015, from http://rntfnd.org/2015/02/11/gps-disruption-halts-portsendangers-ships -us-coast-guard/
- International Maritime Organization (1995/2017). *International Safety Management (ISM) Code*. London: IMO.
- International Maritime Organization (2017). *FAL Convention – convention on facilitation of International Maritime Traffic, 1965, as amended.* London: IMO.
- International Maritime Organization (2017). *Guidance on Maritime Cyber Risk Management - MSC-FAL. 1/Circ. 3.* London: IMO.
- International Maritime Organization (2002). *International Ship and Port Facility Security Code (ISPS).* London: IMO.
- International Maritime Organization (1974). *International Convention for the Safety of Life at Sea (SOLAS)*. London: IMO.
- International Maritime Organization (2002). *International Ship and Port Facility Security Code (ISPS)*. London: IMO.
- Kramek, J. (2013). *The critical infrastructure gap: U.S. port facilities and cyber vulnerabilities.* Federal Executive Series Policy Papers, Brookings Institution.
- MORS (2019). *Kritična infrastruktura.* Retrieved March 01, 2020, from: http://mo.arhiv-spletisc.gov.si/ si/delovna_podrocja/kriticna_infrastruktura/
- Orsosz, M., Chen, J., Maya, I., Salazar, D., Chatterjee, S., Wei, D. (2010). *Protecting our nation's ports with the port security risk analysis and resource allocation system (PortSec 3.0*), Proceedings IEEE Conference on Technologies for Homeland Security (HST), pp 264-269.
- Pasternack, A. (2013). *To Move Drugs, Traffickers Are Hacking Shipping Containers*. Motherboard tech by vice. Retrieved March 01, 2020: https://www.vice.com/en_us/article/bmjgk8/ how-traffickers-hack-shipping-containers-to-move-drugs

- Roberts, F. (2015). *The little-known challenge of maritime cyber security*, in IISA 2015 – 6th International Conference on Information, Intelligence, Systems and Applications [7388071]. Institute of Electrical and Electronics Engineers Inc.
- *Uredba o evropski kritični infrastrukturi* (2011). Official Gazette of the Republic of Slovenia № 35/2011 of 13 May 2011.
- *Regulation (EC) of the European Parliament and of the Council on the implementation of the International Safety Management Code within the Community and repealing Council Regulation (EC) № 3051/95*. Regulation of the European Parliament and of the Council № 336/2006 of 15 February 2006.
- *Regulation (EU) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* Regulation of the European Parliament and of the Council № 2016/679 of 27 April 2016.
- *Regulation (EC) of the European Parliament and of the Council on enhancing ship and port facility security*. Regulation of the European Parliament and of the Council № 725/2004 of 31 March 2004.
- *Zakon o kritični infrastrukturi* (2017). Official Gazette of the Republic of Slovenia № 75/2017 of 22 December 2017.
- *West Coast Port Congestion Could Cost Retailers $36.9 Billion in the Next 24 Months*. Business Wire. Retrieved Feb. 7, 2015, from: http://www.businesswire.com/news/home/ 20150207005007/en/ West-Coast-Port-Congestion-Cost-Retailers36.9#.VPiNIsbA7c8.

A brief presentation of the authors:

Dr Andrej Androjna has been involved in maritime security-related issues for three decades. As a Navy Commander, he has served in various positions and held functions of Staff and Command in Slovenia, abroad and on operations. He is now Head of the Maritime Studies Department at the Faculty of Maritime Studies and Transport, University of Ljubljana.

He has worked across diplomatic, strategic, operational and tactical levels in NATO (Supreme Headquarters Allied Powers Europe (SHAPE), NATO Headquarters Northwood, NATO Headquarters Skopje, KFOR, ISAF) and the EU, where he was thoroughly involved in NATO defence policy issues and the EU Common Security and Defence Policy (CSDP).

His published research covers international and domestic maritime policy and maritime security and safety, while his principal fields of interest include safety of navigation, safety at sea, human resource management, bridge team management and maritime cyber security.

Professor Dr Elen Twrdy has a PhD in Transport Technology at University of Ljubljana. She obtained an MSc in 1995 from the University of Rijeka, Croatia, and her PhD from the University of Ljubljana in 2003. She was a Dean of the Faculty of Maritime Studies and Transportation (University of Ljubljana) during the period 2007-2019. Currently she is Head of Department of Transport Technology.

She is a full Professor at the Faculty of Maritime Studies and Transport at the University in Ljubljana at the first, second and third levels of study. She has written various academic and research papers from the field of transport technology and transport logistics, with a special research area in terminals, ports and maritime transport, and maritime logistics. Her bibliography lists more than 100 papers published in scientific journals and presented at conferences.