【欧州】【海事】

Maritime Issues - Cyber security: ENISA publishes study for improving port-side cyber security

Andrea Antolini Former Researcher JTTRI

【概要：Summary】

Digitalization of the transport system makes transport also more vulnerable to cyber risks. Accordingly, cyber security is a subject of importance also for maritime transport and in particular for autonomous vessels. However, the introduction of shipping connectivity and digital technologies is a relatively recent development in maritime transport, compared to other sectors. Consequently, the maritime sector is still lagging behind in taking measures to improve shipside cyber security. However, since the digitalization has also an increasing impact on the maritime transport, cyber security is becoming more important than ever for ships and ports. There are about 50,000 operating ships in the maritime transport sector, which potentially could become exposed to cyber attacks. The ships' vulnerability to cyber threats and attacks needs to be analysed and measures need to be taken.

The EU's Agency for Cyber security (ENISA) has been working with the EU institutions on problems of the European cyber security issues since 2004. Since 2019, ENISA has been drawing up cyber security certification schemes. ENISA develops advice and recommendations on good practice in information security and it assists EU Member States in implementing relevant EU legislation. The main aim is to improve the resilience of Europe's information infrastructure and networks against cyber threats and attacks.

However, not only ships, but also ports have to consider an improvement of cyber security. For a number of years, ports have been undergoing a digital transformation in order to meet emerging challenges, optimise existing processes and introduce new capabilities, such as automation. The ports' digitalisation has been centred on the inter-connectivity of Information Technology (IT) and Operation Technology (OT) assets and the introduction of new technologies like cloud computing, big data and Internet of Things (IoT). This digital transformation has also led to a change in the cyber risk profile.

Consequently, also cyber security of ports should be viewed as a key factor. There should be an increase in the awareness about cyber security at the ports' board and staff level. Furthermore, port authorities and terminal operators should improve information sharing on cyber threats or cyber incidents as well as good practices amongst port operators and between port operators and other maritime stakeholders, such as shipping companies. Sharing information on cyber threats or cyber incidents as well as good practices is key in improving the overall cyber security posture of the sector, especially in the current situation, in which port stakeholders are facing more and more cyber security challenges with the emergence of new threats, regulations and increased digitalisation. Major incidents such as ransom-ware

attacks targeting ports can have a considerable impact on the security and economy. Accordingly, ENISA has published a new report, which focuses on the evaluation of the cyber threat situation and offers good practices to address those threats for ports. In fact, ports must address cyber security as a top priority to ensure their safety, security, compliance and commercial competitiveness, while unlocking the full capabilities of their digital transformation.

The main objectives of the ENICA study are to build a baseline of good practices to ensure the cyber security of the maritime ports' ecosystem across the EU and to raise awareness of threats and cyber security challenges.

【記事：Article】

1. Background of efforts to improve cyber security in maritime transport

In the maritime and offshore industry, Internet of Things (IoT) sees rising interest and is considered as one of the key digital trends to bring a positive development, along with the development of autonomous and unmanned vessels, block chain, and artificial intelligence. While IoT is the leading digital technology for businesses in all sectors, it only can bring significant value when the issues surrounding cyber security are considered in the utilisation of IoT. The digitalization of the maritime transport sector makes the about 50,000 operating ships a potential target to cyber threats and cyber attacks. In addition, ships can be attacked through data connections with the land-based services. In the linkage between on-board and terrestrial systems, the cyber security of the ship is also dependent on the cyber security of the land-based infrastructure. Therefore, the increased connectivity of modern ships to on-shore via networks makes on-board systems especially vulnerable to cyber attacks. In order to prevent unauthorized access or cyber attacks, not only the ships' cyber safety and security needs to be improved, but also the ports' cyber security.

In the EU, ports play a crucial role at different levels for many sectors and they are a main vehicle for European imports and exports with the rest of the world. Ports are also important nodes for passengers and vehicles transportation (inter and extra-EU). While ports have traditionally been concerned with physical security and safety, they must now integrate cyber security in their security strategy. The global shipping industry is considered being a decade behind other sectors regarding the improvement of cyber security. However, the shipping industry and the port authorities and operators have realised the need to take measures for improving their cyber security.

2. IMO guidelines and codes on cyber security

The International Maritime Organisation (IMO) has started to consider appropriate regulations when it comes to cyber security. In 2017, the IMO amended two of its general security management codes to include cyber security. The International Ship and Port Facility Security Code (ISPS) and the International Security Management Code (ISM) detail how port and ship operators should conduct risk management processes. In June 2017, the IMO's Maritime Safety Committee (MSC) adopted Resolution MSC.428(98) incorporating Maritime Cyber Risk Management into the ISM Code in order to raise the profile and importance of protecting ships. In July 2017, the IMO published the "Guidelines on Maritime Cyber Risk Management" in addition to the resolution on Maritime Cyber Risk Management in Safety Management Systems. Making cyber security an integral part of these processes should ensure that operators are more conscious about cyber risks and threats. Amendments to the ISM and ISPS will come into force on 1 January 2021 and ship owners will have to include cyber security in the ISM Code safety management on ships by that date. The cyber risks should be appropriately addressed in the Safety Management Systems (SMS) no later than the first annual verification of the Document of Compliance (DOC) after 1 January 2021. Thereby, the IMO has decided to include mandatory cyber security requirements into the International Safety Management Code ISM.

3. ENISA initiatives regarding improvement of portside cyber security

The continuous evolution of the transport sector and the introduction of digital technology, along with the development of autonomous and unmanned vessels have increased the importance of cyber security also in maritime transport. The EU's Agency for Cyber security ENISA is actively contributing to European cyber security policy, supporting Member States and EU stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. Therefore, ENISA organised the first Transport Cyber security Conference in cooperation with the European Commission (DG MOVE), the European Aviation Safety Agency (EASA), the European Union Agency for Railways (ERA) and the European Maritime Safety Agency (EMSA) on 23 January 2019.

The global digitalization trend and recent policies and regulations require ports to face new challenges with regards to information and communication technology (ICT). Ports tend to rely more on technologies to be more competitive, comply with some standards and policies and optimize operations. This brings also challenges in the area of cyber security for both, the Information Technologies (IT) and Operation Technologies (OT). Specifically, the emergence of the "SmartPorts" concept brings new challenges for the deployment of emerging technologies (IoT, block-chain, big data, cloud, automation, AI etc.), which often leads to greater exposure of port systems to cyber threats.

Accordingly, the ENISA study entitled "Port Cyber security - Good practices for cyber security in the maritime sector", which was developed together with several EU ports and published in November 2019, intends to provide a useful foundation, on which port authorities and terminal operators can build their cyber security strategy. The study describes key cyber-attack scenarios that could impact the ports ecosystem and identifies main measures to serve as good practices for people responsible for cyber security implementation.

The ENISA report aims to serve as a reference document for stakeholders involved in port cyber security to promote collaboration on maritime port ecosystems across the EU and raise awareness of the relevant threats. The main objectives of the study are to build a baseline of good practices to ensure cyber security of port systems and services, while mapping the relevant cyber security challenges and threats and highlighting some attack scenarios.

This report identifies the existing challenges, in relation to critical operations, stakeholders' ecosystem and assets identification. It then lists the main threats posing risks to the port ecosystem and describes key cyber attack scenarios that could impact them. In particular, the report intends to identify the main port infrastructure and services (maritime cargo, passenger and vehicle transport, fishing activities), and it intends to establish an overview of stakeholders involved in port ecosystems and to define a comprehensive asset taxonomy. It defines a complete threat taxonomy that lists the different threats and their possible impacts. The report also describes cyber-attack scenarios that the port ecosystem could face, influenced from cyber-attacks that have already occurred in the maritime sector. It provides a list of cyber security measures that highlight best practices and helps to improve the cyber security maturity of port ecosystems.

It is a complex environment regarding both, the port landscape in terms of involved stakeholders and the communication flows and system interactions, but also in terms of the evolving IT and OT environment. Finally, the report provides a list of practical baseline security measures to strengthen cyber security in port operations and systems.

An additional important element of the study is to map port services and systems through a high-level reference model to set the scope of the work to be done and serve as a basis for future developments.

The main measures identified are described and intend to serve as good practices for people responsible for cyber security implementation in Port Authorities and Terminal Operators. The report intends to provide

them with a useful foundation on which entities involved in the port ecosystem, especially port authorities and terminal operators can build their cyber security strategy. Furthermore, the study can also be useful for other stakeholders in the broader community within the port ecosystem, such as shipping companies and maritime policy makers.

However, port authorities and terminal operators responsible for port cyber security are encouraged to go beyond the good practices proposed in the ENISA document. The responsible persons should define clear governance around cyber security at port level, involving all stakeholders within port operations. Many companies are involved in port operation and it is crucial to ensure they are all involved in cyber security and aware about how they participate to the global port operation security.

The responsible persons should enforce the technical cyber security basics, like network segregation, updates' management, password hardening, segregation of rights, etc. In the context of OT, network segregation and password protection are key to ensure a correct level of cyber security. Responsible persons should also consider security by design in applications, especially as ports use many systems, some of which are opened to third parties for data exchange, which causes higher levels of vulnerability to the port systems.

The responsible persons should enforce detection and response capabilities at port level to react as fast as possible to any cyber attack before it impacts port operation, safety or security. Ports can rely on simple detection measures such as alerts when a specific action is done (authentication attempt on a very critical asset for example) or search for Indicators of Compromise (IOC), or on more comprehensive, using machine learning to correlate information and identify compromising patterns. Such initiatives have already started to rise within the ports' ecosystems. Furthermore, authorities and terminal operators should improve information sharing amongst port operators and between port operators and other maritime stakeholders, such as shipping companies. Sharing information on threats, incidents and good practices is key in improving the overall cyber security posture of the sector and several proven models, such as a NGO Information Sharing and Analysis Center, ISAC, which provides a central resource for gathering information on cyber threats to critical infrastructure and provides two-way sharing of information between the private and public sector. It can be adapted to provide tangible results.

The port operators and other maritime stakeholders should also address cyber security in the supply chain. In this context, several good practices can be adopted or investigated, including cyber security certification of critical components, well-defined supplier obligations for the entire lifecycle of products/services and specific provisions for supply chain management etc.

Finally, the integration of interdependencies of cyber security risks in the overall cyber risk management process should account for the multiple and complex interconnections of ports with other sectors.

According to ENISA's Executive Director, Juhan Lepassaar, it is important to equip EU ports with all necessary tools and knowledge to address cyber security concerns as they undergo their digital transformation. The report aims to provide port authorities and terminal operators with a comprehensive set of good practices. Given the economic importance of ports in EU trade, the protection of port operations against cyber-attacks becomes paramount.

4. Further ENISA measures: Maritime Cyber security Workshop

On 26 November 2019, ENISA organised a workshop in Lisbon with the objective of strengthening the cyber security of EU ports. The workshop was hosted by the European Maritime Safety Agency (EMSA) and brought together over 60 stakeholders from the EU maritime sector, such as port authorities, terminal operators, shipping companies and national competent authorities. The speakers at the workshop included presentations

from DG CONNECT, DG MOVE and EMSA, as well as speakers from maritime operators, the industry and experts from Information Sharing and Analysis Centres (ISACs). A significant part of the workshop was dedicated to a discussion on ENISA's "Port Cyber security - Good practices for cyber security in the maritime sector report". The workshop participants exchanged views on the key findings of the report and voiced their opinion on what they would like to see ENISA working on next in the maritime sector.

The afternoon session focused on the concept of Information Sharing and Analysis Centres (ISACs), including presentations on good practices and lessons learnt from similar initiatives in other sectors. Subsequent discussions focused on the specific needs of the maritime stakeholders for such an information-sharing platform specifically for the EU maritime sector and on how ENISA could support the creation of a EU maritime ISAC.

5. Conclusion and outlook

The ENISA study on Port Cyber security - Good practices for cyber security in the maritime sector lists an extensive set of security measures that port authorities and terminal operators can adopt to develop a security baseline within the ports' ecosystem. Developed in collaboration with several EU ports, it could be a useful reference document and provide good practices for people responsible for cyber security implementation in Port Authorities and Terminal Operators within the port ecosystem, but also for shipping companies and maritime policy makers.

Regarding the next steps, it will be important to further raise the awareness about cyber security at board and staff level, information sharing amongst port operators, addressing cyber security in the supply chain and integrating cyber security risks in the overall cyber risk management process. While people responsible for port cyber security are encouraged to go beyond the good practices proposed by the ENISA report and to address additional topics, ENISA intends to keep playing its role in the process of strengthening the cyber security of the EU maritime sector in the following years.

References:

https://www.enisa.europa.eu/about-enisa, retrieved 20 December 2019

ENISA: Port Cyber security - Good practices for cyber security in the maritime sector. In: https://www.enisa.europa.eu/publications/port-cyber security-good-practices-for-cyber security-in-the-maritime-sector, November 26, 2019, retrieved 16 December 2019

ENISA: 1st Transport Cyber Security Conference. In: https://www.enisa.europa.eu/events/first-transport-cyber-security-conference, January 23, 2019, retrieved 20 December 2019

ENISA: How can EU ports tackle new cyber threats? In: https://www.enisa.europa.eu/news/enisa-news/how-can-eu-ports-tackle-new-cyber-threats, 26 Nov 2019, retrieved 16 December 2019

ENISA organises Maritime Cyber security Workshop in Lisbon. In: https://www.enisa.europa.eu/news/enisa-news/enisa-organises-maritime-cyber security-workshop-in-lisbon, November 27, 2019, retrieved 17 December 2019

Guidelines on maritime cyber risk management. In: https://safety4sea.com/guidelines-on-maritime-cyber-risk-management/, retrieved 10 Sept. 2019

How can EU ports tackle new cyber threats? In: https://www.enisa.europa.eu/events/first-transport-cyber-security-conference, November 26, 2019, retrieved 18 December 2019

IMO: THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS. In: http://www.imo.org/en/OurWork/Facilitation/Electronic%20Business/Documents/guidelines-on-cyber-security-onboard-ships.pdf, retrieved 9 Sept. 2019

IMO: GUIDELINES ON MARITIME CYBER RISK MANAGEMENT, MSC-FAL.1/Circ.3, 5 July 2017 in: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf, retrieved 10 Sept. 2019

IMO MSC: RESOLUTION MSC.428(98) (adopted on 16 June 2017) MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS. In: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf, retrieved 10 Sept 2019

Maritime industry publishes updated guidelines for cyber security on ships. In: 10/12/18 https://safety4sea.com/maritime-industry-updates-guidelines-for-cyber-security-on-ships/, 10 Sept. 2019

Martin, Keith/ Hopcraft, Rory: 50,000 ships worldwide are vulnerable to cyberattacks. In: https://www.independent.co.uk/life-style/gadgets-and-tech/ships-cyberattacks-vulnerable-worldwide-a8404191.html, 20 June 2018, retrieved 10 Sept. 2019

The future of Maritime Cyber security. In: https://securestatecyber.com/cyberbloggen-en/the-future-of-maritime-cybersecurity/, April 15, 2019, retrieved 30 December 2019