Dino Gliha*

MARITIME CYBER CRIME - 21ST CENTURY PIRACY

SUMMARY

Maritime industry is the backbone of international trade and the global economy. Around 80 per cent of global trade by volume and over 70 per cent of global trade by value are carried by sea and are handled by ports worldwide. With the development of digital technology, same assome other industries, maritime sector has faced with problem of cyber security. Some efforts in dealing with that issue have been taken by certain private and public maritime organizations. However, they have not shown to be sufficient. Therefore, to face with the issue of cyber threats, creation of a comprehensive legal framework is needed. In lack of prior legal solutions, useful analogy may be drawn with regulation of piracy on high seas as a guidance for creation of universal legal framework on cyber security.

Key words: cyber security, maritime sector, cargo transportation, piracy, NIS Directive

INTRODUCTION

With the 21st century development of industry and technology, there is a constant tendency on increasing dependence on digital technology.However, alongside to all the benefits that were developed with digital revolution, it has also opened a whole new issue of cyber security among different industries. Maritime sector, as being one of the most involved industries in worldwide economy, is certainly one of them. Especially, cargo transportation system has suffered a series of cyber-attacks.

However, instead of taking a proactive prevention approach in dealing with cyber security issue, maritime sector has shown to be reactive in setting standards and procedures based on catastrophic events. Throughout the last years, through their reports and guidelines, some international public and private organization have taken additional efforts to raise awarenessof potential cyber threats within maritime sector. Although, their activity has an important role in combating maritime cyber piracy, still it is has not shown to be enough.

Therefore, to improve the level of cyber security adequate legal frameworkthat would provide strong basis on global level to fight with this widespread menace is needed. Whereas, in developing of such a comprehensive legal framework particularities of cyber security and maritime sector should be taken into consideration. Moreover, considering the similarities, in creation of such regulation, treatment of piracy on high seas could use as a useful guidance.

* Mag.iur., Legal Trainee/odvjetnički vježbenik, Čačić&Partners, Law Firm/odvjetničko društvo.

One step closer of achieving that goal may be theEuropean Union's (hereinafter: EU) Directive on Security of Network and Information Systems[1] (hereinafter: the NIS Directive). The NIS Directive was adopted in 2016 and it is the first EU's directive that deals with issue in matter.

Considering abovementioned, this paper will present overview of current cyber security status in maritime sector and analyse possible legal solutions in order to deal with this widespread issue.

1. CYBER CRIME IN MARITIME SECTOR

Maritime transport industry is the backbone of international trade and the global economy. Around 80 per cent of global trade by volume and over 70 per cent of global trade by value are carried by sea and are handled by ports worldwide.[2] With the emergence of big data and increasingly interconnected technologies throughout last two decades, maritime industry is going through a digital revolution.[3] Some of the new developments are GPS navigation, real-time weather data feeds as well as smart containers, and this is just the beginning. There is a constant tendency of increasing the size of ships and decreasing the number of crew and other persons involved.[4]

However, increased dependence on digital technology can result in increased potential vulnerability and risks within maritime industry sector.[5] That relates especially to logistics and transportation systems where information is often shared among wide variety of different subjects. Attack on any part of those systems could, and already has, lead to catastrophic consequences.[6]

Earliest known cyber maritime incident was in 2001 when a teenager carried out denial of service (hereinafter: Ddos) attack on the computer system at port of Houston.[7] Although there were no severe consequences as a result of a performed attack, this incident aroused several issues. Firstly, vulnerability of computer systems in maritime industry and secondly question of liability for conducting such act.Namely, charged individual walked away free from the incident despite the fact it was determined that act was performed by his computer.[8]

---

[1] Directive (Eu) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp 1–30.

[2] United Nations Conference on Trade and Development, Review of Maritime Transport 2015, *http://unctad.org/en/PublicationsLibrary/rmt2015_en.pdf*(April 17, 2017), 48.

[3] Digitalisation in shipping and logistics, *https://www.munichre.com/en/reinsurance/magazine/topics-online/2015/09/digitalisation-shipping-logistics/index.html* (April 17, 2017)

[4] J. Wagstaff, All at sea: global shipping fleet exposed to hacking threat, Reuters, April 24, 2014, *http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424* (April 17, 2017)

[5] S. L. Caponi, K. B. Belmont, Maritime Cybersecurity: A Growing Threat Goes Unanswered, Intellectual Property & Technology Law Journal, Vol 27, No 1, January 2017, 17

[6] M. G. Burns, Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience, CRC Press, Taylor & Francis Group, Boca Raton, 2016, 193.

[7] B. van Niekerk, Analysis of cyber-attacks against the Transportation Sector, in: Maximiliano E. Korstanje, Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities, IGI Global, Hershey, 2017, 71.

[8] S. W. Brenner, B. Carrier, J. Henninger, The Trojan Horse Defense in Cybercrime Cases, Santa Clara High Technology Law Journal, Vol 21, Iss 1, 3-6

Attack on port of Houston had been a clear alert for transport and maritime industry to improve their cyber security systems and their general awareness of cyber threats. However, improvements were not sufficient and number of attacks followed. Although, there are not so many noted cyber-attacks, it is evident that real numbers are much bigger.[9] Namely, companies in transport and maritime industry tend not to report cyberincidents due to potential loss of their reputation or lack of knowledge they had been attacked.[10]

In upcoming years several other cyber maritime incidents occurred; such as attack on the Iranian shipping line IRISL in 2011 where attacks damaged all the data related to rates, loading, cargo number, date and place,[11]2011-2012 drug smuggling incident within Port of Antwerp,[12] 2012 penetration of Australian Customs and Border protection cargo system software,[13] 2013*Icefog* cyber-attack focused on data extracting from Japanese and South Korean maritime and shipbuilding groups,[14]2013 MODU's cyber incident that paralyzed oil rig in Gulf of Mexico,[15]2016 Port of Oakland Ddos attack on administrative site[16]*etc.*

The motivation for performance of those attacks in maritime sector appears no different than in some other industries. Therefore, some attacks are motivated purely by financial reasons by stealing money directly from maritime companies or for example, to contraband cargo. Other attacks are aimed at potentially infiltrating, controlling, or damaging critical infrastructure, which global shipping industry certainly is in world economy.[17]

Therefore, considering the variety of potential cyber-attack targets there are lots of potential perpetrators behind those incidents. State actors are usually driven by political and strategic goals through cyber espionage, cyber sabotage, and cyberwar fare. Criminal networks and gangs are, in contrast to state actors, motivated usually by financial rewards in order to support their illicit activities. Their targets are mostly commercial organizations. Private companies use

---

[9] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, Copenhagen, 2014, *http://www.sfmx.org/support/amsc/cybersecurity/webdocs/Maritime%20Cyber%20Crime%2010-2014.pdf* (March 28, 2017.), 6.

[10] P. Glass, Why don't maritime companies want to report cyber attacks?, WorkBoat, October 15, 2015, *https://www.workboat.com/blogs/washington-watch/why-are-maritime-companies-reluctant-to-report-cyber-attacks/* (March 28, 2017.)

[11] Y. Torbati, J. Saul, Iran's top cargo shipping line says sanctions damage mounting, Reuters, October 22, 2012, *http://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022* (April 17, 2017)

[12] T. Bateman, Police warning after drug traffickers' cyber-attack, BBC News, 16 October, 2013, *http://www.bbc.com/news/world-europe-24539417* (April 17, 2017)

[13] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, *op. cit.* n 9, 8

[14] Kaspersky lab, The 'Icefog' Apt: A Tale of Cloak and Three Daggers, 2013, *http://media.kaspersky.com/en/icefog-apt-threat.pdf* (April 17, 2017)

[15] S. Swanbeck, Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs, CSIS Strategic Technologies Program, June 22, 2015, *https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities* (March 28, 2017.)

[16] K. K. Belmont, Maritime Cybersecurity: Cyber Cases in the Maritime Environment, July 21, 2016, *http://aapa.files.cms-plus.com/SeminarPresentations/2016Seminars/2016SecurityIT/K.%20Belmont%20-%20AAPA%20Maritime%20Cybersecurity%20FINAL.pdf* (March 28, 2017.), 16.

[17] L. Jensen, Challenges in Maritime Cyber-Resilience, Technology Innovation Management Review, April 2015, *https://timreview.ca/sites/default/files/Issue_PDF/TIMReview_April2015.pdf* (March 28, 2017.), 37.

hacking and cyber-attacks to gain competitive advantage against their competitors or to obstruct concurrent work. Hacktivist tend to promote political ideas and movement and can cause severe problems to targeted organization's continuity of operation and brand. Although, terrorists are not so much focused on cyber-attacks, they still sometimes conduct cyber-attacks on tactical targets. Employees and former employees, as insiders, represent one of the most severe threats to the organizations they worked for since they are introduces with the system from the inside. Finally, lone actors act solely from their own agenda. That category includes disturbed individuals, disgruntled employees or simply persons who act from their pure curiosity.[18]

One of the most threatened area within maritime sector is cargo transportation system, where cyber-attacks are performed to smuggle illegal cargo within containers. Considering the *modus operandi*of the performed attacks, there are different ways for performing them. However, attacks are mostly focused on ports where containers are being transferred on and off the ships. Therefore, following paragraphs will focus on this part of maritime sector and possible solutions on how to face with this problem.

2. CASE STUDY: PORT CYBER SECURITY AND CARGO CONTRABAND

To understand and discuss the issue of cyber-attacks within maritime sector it is necessary to understand *modus operandi* of those attacks. Considering cargo smuggling most severe cyber-attacks that had already occurred were conducted through one of the following types of cyber-attacks: deleting carrier information as to the location of cargo, *Zombie Zero* and*ghost shipping*.

Deleting carrier information as to the location of cargo

In August 2011, Islamic Republic of Iran Shipping Lines (hereinafter: IRISL) suffered an intense cyber-attack.[19] Cyber-attack damaged all the data related to rates, loading, cargo number, date and place, and eliminated company's internal communication network. All of which resulted with situation that containers within where left without any control or knowledge where they really are.[20]

Although, the data was eventually restored and normal functioning of the IRISL system has been recovered, the company suffered some serious consequences. Namely, as a result of disruptions in operating system some cargo was sent to wrong destination which resulted with severe financial losses. Even, more worrisome part was that considerable amount of cargo was lost without trace as a result of the cyber-attack.[21]

A similar attack on a major international container line would have a crippling effect on the supply chains of thousands of international companies.[22]

---

[18] R. Sen, Cyber and Information Threats to Seaports and Ships, in: Michael McNicholas (ed.), Maritime Security: An Introduction, 291-293.

[19] Y. Torbati, J. Saul, *op. cit.* n 11.

[20] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, *op. cit.*, n 9, 6

[21] *Ibid.*

[22] L. Jensen, *op. cit.* n 17, 37

Zombie Zero

Zombie Zero is a so-called attack method,tailor made to attack shipping and logistic companies. It was discovered by a deception technology company TrapX in 2014, after at least eight shipping-and-logistic companies were compromised due to a malware that was preloaded into newly manufactured scanners by a manufacturer in China.[23]

The attack was construed in a following way. When the scanners were plugged into company's network it launched series of automated attacks searching the companies Enterprise resource planning (hereinafter: ERP) financial server. Once the server was found, malware would proceed to compromise the server. Next step consisted of establishing remote connection to a location in China. After the connection was established the perpetrator would gain complete insight into ERP financial system and ability to modify shipping database.[24]

Therefore, compromised scanners gave perpetrators a foothold inside the company's network from which to establish a pivot point, which could be then used to compromise the entire enterprise network. That means that through the weaponized malware, the attackers could bypass most of the company's enterprise perimeter, security measures and compromise the target network almost completely.[25]

Concerning the cargo management system, with successful *Zombie Zero* attack, perpetrators would gain ability to manipulate cargo appearance within certain shipping system which could be also used for cargo contraband.[26]

Although, *Zombie Zero* attacks were later discovered and prevented, the true scope of that attack and its true consequences will never be known, except perhaps to the perpetrator.[27]

Ghost shipping

Probably the most notable cyber incident in maritime transportation system was Port of Antwerp incident that occurred between 2011 and 2013. For two full years, crime organization, with help of Belgian group of hackers, used port of Antwerp for drug smuggling by hiding drugs among legitimate cargo,including timber and bananas shipped in containers from South America.[28]

Namely, cargo management systems include television cameras for automatic container identification and for documentation for insurance purposes. Also,it manages loading and unloading ques, performs billings and more. Belgian hackers cracked those management systems within two piers in port. Which enabled them to locate every container before the real

---

[23] TrapX Research Labs, Anatomy of an Attack - The Discovery of Zombie Zero, March 1, 2017, *http://deceive.trapx.com/WP-AOA-Zombie-Zero_215-Landing-Page.html?utm_source=TrapX&utm_medium=Website* (March 28, 2017.), 5.

[24] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, *op. cit.*, n 9, 7.

[25] TrapX Research Labs, Anatomy of an Attack - The Discovery of Zombie Zero, *op. cit.*, n 23, 7-8.

[26] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, *op. cit.*, n 9, 7.

[27] TrapX Research Labs, Anatomy of an Attack - The Discovery of Zombie Zero, *op. cit.*, n 23, 5 *et* 9.

[28] T. Bateman, *op. cit.* n 12.

client appeared to collect it. Later on, when breach was exposed and the port installed firewalls, hackers physically penetrated into the port and installed wireless bridges on the operating computers that allowed them direct access to the operating system. It took two years before the port find the reason for complete disappearance of containers at the port.

Considering its profoundness and proficiency, after the Port of Antwerp incident, that kind of cyber invasion on cargo management system was coined as *ghost shipping*.[29]

One more incident that could also fall within extent of term*ghost shipping* is maritime cyber incident that occurred within Australian Customs and Border protection in 2012. The perpetrators managed to penetrate Australian Customs and Border protection's software for cargo system that allowed them to check whether their shipping containers with contraband were regarded as suspicious by the police or customs authorities. If their cargoes went unnoticed the group would intercept the shipments, whilst if they sensed that their containers may be at risk, they simply abandoned it.[30]

3. COMBATING CYBER CRIME IN MARITIME SECTOR

After the brief overview of cyber incident in maritime sector was given, it is clear that cyber-attacks are present, real and represent a severe threat towards maritime industry sector. Therefore, it is important to know how to respond to such a threat?

For purpose of prevention of cyber incidents several private and public maritime organizations have published series of documents that deal with the problem of cyber security in maritime sector.

In November 2011, European Agency for Network and Information Security (hereinafter: ENISA) has published the first EU report ever on cyber security challenges in the Maritime Sector.[31]Within its report ENISA had found maritime sector is critical for the European society. However, it also indicated that cyber threats are a growing menace that is rapidly spreading over different industries with potential disastrous consequences for the European Member States' governments and social wellbeing in general. As a conclusion of its audit, ENISA proposed series of observations and recommendationssuggesting the possible approaches that could be taken for addressing cyber risks.[32]

In June 2014, United States Global Accountability Office (hereinafter: GAO) published a report on ports cybersecurity.[33] GAO's objective was to identify the extent to which Department of Homeland Security and other stakeholders have taken steps to address

---

[29] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, *op. cit.*, n 9, 8.

[30] C. R. Hayes, Maritime Cybersecurity: The Future of National Security, Naval Postgraduate School, Monterey, California, thesis, *http://calhoun.nps.edu/bitstream/handle/10945/49484/16Jun_Hayes_ Christopher. pdf? sequence=1&isAllowed=y* (March 28, 2017.), 16.

[31] ENISA, Analysis of Cyber Security Aspects in the Maritime Sector, November 2011, *https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport* (March 28, 2017.)

[32] *Ibid.*1-2.

[33] GAO, Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity, June 2014, http://www.gao.gov/assets/670/663828.pdf (April 02, 2017.)

cybersecurity in the maritime port environment. For that purpose, it examined relevant laws and regulations; analysed federal cybersecurity-related policies and plans; observed operations at three U.S. ports selected based on being a high-risk port and a leader in calls by vessel type, e.g. container; and interviewed federal and non-federal officials. At the end of its audit, GAO concluded that possible disruptions in operation of USA ports could be devastating to the national economy. Although, some actions had been taken by competent bodies in order to prevent that scenario, before all, comprehensive risk assessment that includes cyber threats, vulnerabilities, and potential impacts was needed.[34]

One of the most significant research conducted on maritime cybersecurity is a whitepaper issued by the cybersecurity company CyberKeel in 2014. Through mentioned report, thorough research had been conducted that examined the vulnerability of the maritime industry to various cyber-risks, and highlighted its lack of adequate defences.[35] It is one of the most referred documents within researches that deal with issue in matter.

In February, 2016 BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO have published the Guidelines on Cyber Security Onboard Ships.[36]Guidelines offer guidance to ship-owners and operators on how to assess their operations and develop the necessary procedures and actions to improve resilience and maintain integrity of cyber systems onboard their ships. Although guidelines are not mandatory, they represent a helpful contribution to the work being done to safeguard the shipping industry from the growing threat of cyber-attacks.[37]

Further on, for purpose of raising awareness and on cyber risk threats and vulnerabilities, International Maritime Organization (hereinafter: IMO) issued Interim Guidelines on Maritime Cyber Risk Management.[38] The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

However, although all those papers, among others, have their value and represent improvement in combating cyber threats - still it is too little too late. Namely, all of those researches have shown that maritime industry is vulnerable to cyber-attacks but that very little has been done to prevent or deter them. Most of the actions taken in combating maritime cyber threats were just a post response toward an incident that had already occurred.[39]

---

[34] *Ibid.*, 28.

[35] CyberKeel, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, *op. cit.* n 9.

[36] BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO, The Guidelines on Cyber Security onboard Ships, Version 1.1 – February 2016, *http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14* (April 17, 2017)

[37] W. Lawrence, New industry guidelines for cybersecurity on board ships, July 05, 2016, *http://www.clydeco.com/insight/article/new-industry-guidelines-for-cybersecurity-on-board-ships* (April 17, 2017)

[38] IMO, Interim Guidelines on Maritime Cyber Risk Management, MSC.1/Circ.1526, June 1, 2016, *http://www.imo.org/en/MediaCentre/HotTopics/piracy/Documents/MSC1Circ1526%20%20Interim%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management.pdf*, (April 17, 2017)

[39] C. R. Hayes, *op. cit.* n 30, pp 2.

However, raising awareness and motivating interested subjects to a proactive approach towards cyber-security in maritime sector is a gradual process in which international maritime private and public organizations may have one of the key roles. That role especially shows through their reports and papers, what they are already doing.

However, from legal perspective there is much to be done. Despite abundance of recommendations, reports and proposals, from which some were previously noted, very little has been achieved as to universal agreement in combating cyber threats as well as in maritime sector, as in general. Stillas it can be seen from above, majority of cyber-attacks have been unnoticed or unreported. Moreover, even if certain attack is discovered and processed, there are difficulties in both finding and condemning the responsible actors.

Therefore, considering the specific nature of cyber activities and maritime sector, specific approach should be taken in combating with cyber threats within maritime sector.

4. REGULATION OF CYBER-ATTACKS - A VIEW TO THE FUTURE

One of the ideas that was introduced yet in late 1990s was to treat cyberspace similarly to some other global spaces.[40] Namely,cyberspace, where cyber-attacks are actually conducted, has its own particularities. That mostly refers to its non-physical and universal character from where repercussions are being reflected to physical world. Considering aforementioned, parallel could be drawn to some other areas where effective control was lacking due to unwillingness or inability of States to tackle the problem within their own jurisdiction.[41] That certainly refers to air, space and high seas treatment.

However, considering the particularities of cyberspace with special view on maritime cyber threats, and in lack of better solutions, the best comparison may be drawn with treatment of piracy on high seas. Namely, there are certain important similarities between those two that could be basis for useful analogy in development of a comprehensive framework on international level to combat cyber threats.[42]

Both piracy and cyber-attacks are carried out in an environment where jurisdiction is unclear and their repercussions are often global. Therefore, as United Nations Convention on the Law of the Sea[43] balances the territorial jurisdiction of nations with concept of universal definition, same should be done with treatment of cyber-attacks.[44]

---

[40] D. C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol 4, Iss 1, 83-85.

[41] J. Kalpokiene, Ignas Kalpokas, *Hostes Humani Generis*: Cyberspace, The Sea and Sovereign Control, Baltic Journal of Law & Politics, Vol 5, No 2, 2012, 138-139.

[42] W. M. Stahl, The Unchartered Waters of Cyberspace: Applying the Priniciples of International Maritime Law to the Problem of Cybersecurity, The Georgia Journal of International and Comparative Law, Vol 40, No 1, 2011, 251.

[43] United Nations Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 3; 21 ILM 1261 (1982), *http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf* (April 17, 2017)

[44] *Ibid.*, 267.

Further on, there are problems with defining piracy as well as cyber-crime considering that it is often unclear whether the perpetrators are affiliated with or sponsored by sovereign nations or criminal organizations.[45]

Finally, both cyberspace and high seas, where cyber-attacks and pirate attacks are performed, have become immeasurable trade routes and space of abundant resources, and following objects of political and military struggle among states which in parallel try to protect themselves from potential threats and gain influence on a global scale.[46]

Bearing all aforementioned in mind, analogizing cyber threats to the concerns that spawned cooperation in developing international maritime law is a useful starting point for analysing and developing necessary international response to combat with issue of cyber security.[47]

One step closer of achieving that goal is certainly adoption of Directive on security of network and information systems (the NIS Directive) by the European Parliament on 6 July 2016.[48]

The NIS Directive represents the first EU-wide rules on cyber security with main objective to achieve high common level of security of network and information system within European Union by means of: improved cyber security capabilities on national level, increased EU-level cooperation, risk management and incident reporting obligations for operators of essential services and digital service providers.[49]

For purpose of achieving its goals, on national level the NIS Directive obliges Member States to adopt national strategies on the security of network and information system, to designate national competent authorities to monitor implementation of the NIS Directive provisions on national level and to ensure cross border cooperation, and to designate Computer Security Incidents Response Teams (hereinafter: CSIRTs) which would deal directly with cyber breaches.[50]

Further on, the NIS Directive predicts creation of so called Cooperation Group and CSIRTs Network that will promote joint cooperation in improvement of cyber security.[51] In light of aforementioned comparison with maritime piracy regime, this could be compared to global duty of cooperation in the repression of piracy in Art 100 of the UNCLOS where: *All states shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State.*

---

[45] *Ibid.* pp *268.*

[46] J. Kalpokiene, I. Kalpokas, *op. cit.* n 41,156-157.

[47] W. M. Stahl, *op. cit.* n 42, 273.

[48] Directive (Eu) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, 1–30

[49] Directive on Security of Network and Information Systems, EU Commission Press Release, July 6, 2016, *http://europa.eu/rapid/press-release_MEMO-16-2422_en.htm* (April 17, 2017)

[50] NIS Directive Art 8 *et* 9.

[51] NIS Directive Art 11 *et 12.*

Moreover, water transport sector, which can be compared to what is referred to as maritime sector within this paper, is recognized as one of the essential services with an important role for the society and economy. As such, the NIS Directive gives certain subjects of water transport sector some additional obligation that are focused primarily on improvement of security measures. Also, the NIS Directive prescribes obligation for operators within water transport sector to report all cyber incidents, which is one of the severe problems in current regime of cyber security due to non-reporting of incidents for different reasons.[52]

However, although, European Union initiative is a giant leap towards fighting cyber-crime, this should only be looked as a starting point in development of comprehensive system of fighting maritime cyber-crime, and cyber-crime in general. Namely, the NIS Directive is mostly focused on improvement of cooperation among Member States of EU and improvement of cyber security status on national level and it does not create universal jurisdiction for processing cyber-crimes.That means that there is still no global approach on fighting cyber threats and the success of the NIS Directive will depend mostly on States and other interested subjects.[53]Also, the NIS Directive extends only to EU Member States, although it predicts possible international cooperation on global level in Art 13. Moreover, in near future idea of creating an international tribunal for cyber-crime activity should also be looked. Employing an international tribunal of that kindwith universal jurisdiction would contribute to equal treatment of offences across jurisdictional lines and would also deter cyber-attacks and provide a venue for prosecution where nations otherwise often refuse to prosecute such acts.[54]

CONCLUSION

Cyber security within maritime sector is clearly a severe issue that must be dealt with as soon as possible. Maritime sector is an essential part on worldwide economy and every attack on it may have disastrous global consequences. However, it has shown to be especially vulnerable to cyber threats.

Certain private and public maritime organizations have given most of efforts in addressing stakeholder of this issue. However, global approach is needed. There is an urgent need of comprehensive legal framework on global level that will deal with issue of cybersecurity, as well as in maritime sector as in general. Useful starting point in achieving that goal may be use of analogy with regulation of piracy on high seas. Namely, increased cooperation among states and universal jurisdiction seems like right solutions in combating cyber threats.

The European Union has made a step forward with adoption of the NIS Directive. However, the NIS Directive is mainly focused on increase of cyber security on national level of its Member States and, therefore, it should be looked only as a commencement in procedure of creating universal legal system for fighting cyber threats. Without that kind of system, cyber incidents will continue to occur within maritime sector, as well in other parts of industry.

---

[52] NIS Directive Art 14 in accordance with Preamble para 10.

[53] Possible international cooperation with third parties or international ogranizations through Cooperation Group is predicted in Art 13 of NIS Directive.

[54] W. M. Stahl, *op. cit.* n 42, 272.

SAŽETAK

POMORSKI CYBER KRIMINALITET - PIRATSTVO 21. STOLJEĆA

Pomorska industrija je oslonac međunarodne trgovine i globalne ekonomije. Oko 80% globalne trgovine po volumenu i 70% globalne trgovine po vrijednosti obavlja se morem i prolazi kroz luke diljem svijeta. Razvojem digitalne tehnologije, kao i drugih grana industrije, pomorski sektor suočio se s problemom sajber sigurnosti. Određene privatne i javne organizacije poduzele su napore pri suzbijanju problema sajber sigurnosti. Međutim, dosad uloženi napori nisu se pokazali dostatnima. Naime, da bi se riješio problem sajber sigurnosti za početak je potrebna izgradnja sveobuhvatne pravne regulative na tom području. Za to vrijeme korisna analogija može se povući s regulacijom piratstva na otvorenom moru kao smjernicama za razvoj univerzalnog pravnog okvira za sajber sigurnost.

Ključne riječi*:* sajber sigurnost, pomorski sektor, prijevoz tereta, piratstvo, NIS Direktiva.