TRANSNAV
http://www.transnav.eu

the International Journal
on Marine Navigation
and Safety of Sea Transportation

Volume 13
Number 1
March 2019

DOI: 10.12716/1001.13.01.24

Raising Awareness on Cyber Security of ECDIS

B. Svilicic, D. Brčić, S. Žuškin & D. Kalebić
University of Rijeka, Rijeka, Croatia

ABSTRACT: In the maritime transport, the Electronic Chart Display and Information System (ECDIS) has been developed into a complex computer-based ship critical operational technology system, playing central roles in the safe ship navigation and transport. While ECDIS software maintenance is regulated by the International Maritime Organization (IMO) ECDIS performance standards and related circulars, underlying software and hardware arrangements are implemented by ship-owners and supported by ECDIS equipment manufacturers. In this paper, we estimate ECDIS cyber security in order to study the origin of ECDIS cyber security risks. A set of ECDIS systems is examined using an industry-leading vulnerability scanning software tool, and cyber threats regarding the ECDIS backup arrangement, underlying operating system and third party applications are studied.

1 INTRODUCTION

Ship operational technology systems for a last two decades have been intensively developed by means of digitalization, integration and networking. The development resulted in complex and computer-based technology systems, and therefore there is urgent need for safeguarding shipping from cyber threats and vulnerabilities (Svilicic et al. 2019, Tam et al. 2019, Filic 2018, Kessler et al. 2018, Polatid et al. 2018, Hareide et al. 2018, Shapiro et al., 2018, Svilicic et al. 2018, Lee et al. 2017, Hassani et al. 2017, Burton 2016, Balduzzi et al. 2014, Svilicic et al. 2005). The International Maritime Organization (IMO) has recently published the Guidelines on high-level recommendations for maritime cyber risk management (IMO MSC-FAL.1/Circ.3 2017), and imposed to include cyber risk assessment in the implementation of the International Safety Management (ISM) Code safety management system on ships by 1st of January 2021 (IMO MSC.428(98) 2017).

The Electronic Chart Display and Information System (ECDIS) is considered as a critical operational technology for voyage planning and accepted as complying with the updated paper charts (complies with IMO regulations and the mandatory carriage), and plays central roles in the safe ship navigation and transport (IMO MSC.1/Circ.1503/Rev.1 2017). However, ECDIS is basically a software package installed on a conventional personal computer with a conventional operating system pre-installed. The ECDIS software is designed to be flexible regarding to the underlying operating system. The flexibility allows solving of interlinking and controlling issues that rise from the usage of various specific operational technology assets and conventional information technology assets. While maritime regulations and policies govern ECDIS software maintaining (IMO MSC.1/Circ.1503/Rev.1 2017, IMO 2010), adequate arrangements of the underlying software and hardware is implemented by shipowners and supported by ECDIS equipment manufacturers.

Recently, we presented a cyber security risk assessment of a ship and utilization of a cyber vulnerability scanner software tool (Svilicic et al. 2019). In this paper, we estimate ECDIS cyber security in order to study the origin of ECDIS cyber security risks. Cyber vulnerabilities of a set of ECDIS systems has been examined by performing computational vulnerability scanning using an industry-leading software tool. Cyber threats regarding the ECDIS backup arrangement, the underlying operating system and third party applications are studied. The cyber risk level of the ECDIS systems has been estimated by a qualitative analysis of the cyber threats identified.

2 THEORY

2.1 *ECDIS background*

The ECDIS is officially accepted by IMO as meeting carriage requirements onboard SOLAS vessels, representing an equivalent to paper navigational charts and performing as a mandatory and primary navigation mean (IMO MSC.282(86) 2009). According to the on-board fulfillment requirements, the ECDIS system is to be type approved, with implemented up-to-date Electronic Navigational Charts (ENCs), ECDIS software maintained, and installed with adequate back-up arrangement (IMO MSC.1/Circ.1503/Rev.1 2017, IMO MSC.282(86) 2009, IHO 2017, IHO 2018). According to the IMO performance standards, the system consists of three mandatory sensors (position, heading and speed source) that are connected directly to the ECDIS system (Brčić et al. 2015). In addition, the ECDIS enables fusion of additional sensors regarding navigation environment and ship's safety. Timely updating of ENC also ensures reliable ECDIS performance and represents a basic prerequisite for safe navigation. The ENCs are commonly updated with portable storage devices and much rarely via an Internet connection. Figure 1 shows a typical configuration of ship ECDIS system.

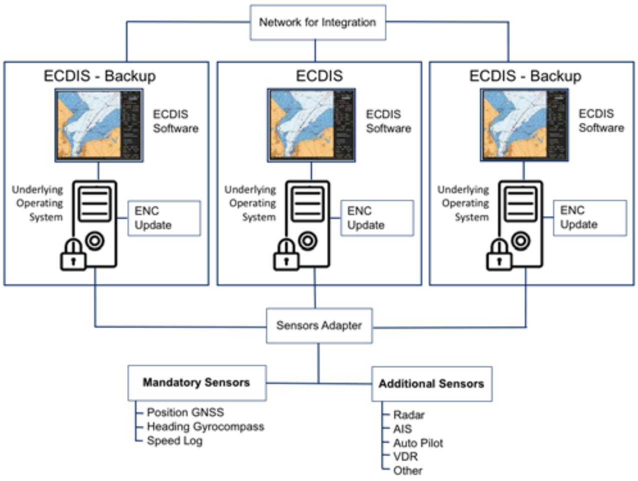


Figure 1. A typical configuration of ship ECDIS system.

The ECDIS backup arrangement is regulated by the IMO performance standards to ensure safe navigation in case of an ECDIS failure (IMO SOLAS 2014, IMO MSC.232(82) 2006, IMO MSC.282(86) 2009). The function of a backup ECDIS system is to enable safe takeover of the ECDIS functions, as well as to ensure safe navigation for the remaining part of the voyage.

Computational vulnerability scanning

The computational vulnerability scanning is a process of reviewing a targeted host (in our case ECDIS) to locate and identify known weaknesses. The vulnerability scanning process is shown on Figure 2. The process starts with gathering all relevant technical information about the targeted host and network configuration. In the second phase, a vulnerability scanning software tool setup is performed by defining IP addresses of the targeted hosts, activating adequate scanning plugin database with known vulnerabilities, and defining appropriate credential to gain adequate access to the targeted hosts. As a result of the vulnerability scanning, a report is generated including vulnerabilities detected descriptions coupled with recommended solving actions.

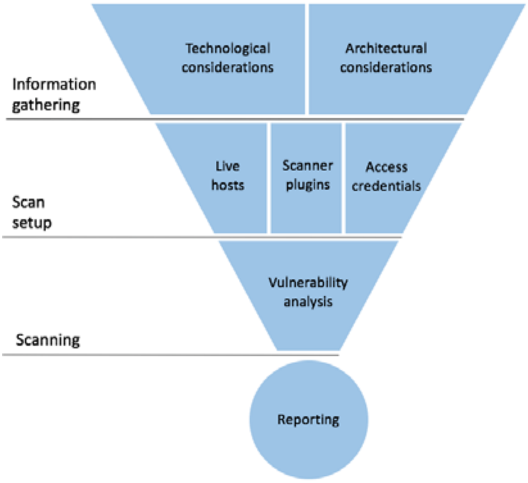


Figure 2. Computational vulnerability scanning process.

The computational vulnerability scanning is commonly conducted using commercial tools. Table 1 shows a list of today's mostly used software tools together with the operating system and license type.

Table 1. Vulnerability scanning software tools.

Name	Operating System	License
Nessus	Cross-platform	Proprietary
Kali	Linux	Free
ImmuniWeb	MS Windows	Proprietary
Netsparker	MS Windows	Proprietary
Acunetix	Cross-platform	Proprietary
Nexpose	Cross-platform	Free
Core Impact	MS Windows	Proprietary
OpenVAS	Linux	Free
Retina	MS Windows	Free

Usage of these tools allows scanning a large number of hosts for known vulnerabilities but is limited to detect only vulnerabilities for which the vendor has released the plugin.

3 EXPERIMENTAL DETAILS

The vulnerability scanning of the Transas Navi-Sailor 4000 ECDIS was performed (Transas, 2018). The ECDIS is installed and used as a simulator for studying purposes at the Faculty of Maritime Studies University of Rijeka. While the Transas ECDIS functional differences between the ECDIS software used on ships and for simulators are related only to interlinking with the active sensors, the underlying hardware and software, particularly the operating system, are the same.

The cyber vulnerability estimation of the ECDIS was performed using the Nessus Professional vulnerability scanner version 8.0.1 (Nessus, 2018). A laptop with the pre-installed Nessus Professional vulnerability scanner has been connected to a local network with the six ECDIS stations connected. The testing setup is shown on Figure 3.

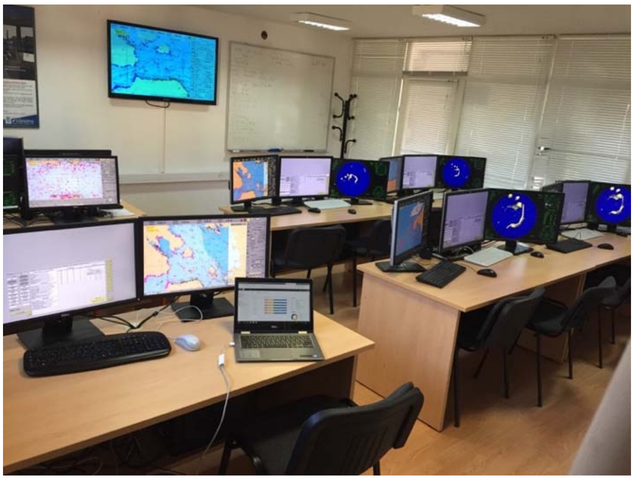


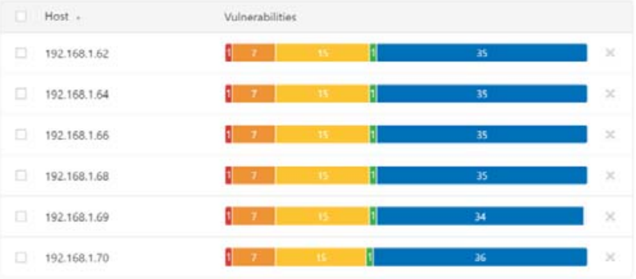
Figure 3. Testing setup for ECDIS vulnerability scanning.

The Nessus Professional vulnerability scanner was configured to automatically scan all of the ECDISs, and setup to run plugins for Microsoft Windows operating systems, web server applications, and miscellaneous services. While the ECDIS software was running under administrative credentials, the remote vulnerability scanning was performed without administrative privileges. The ECDISs under the test are connected in a separated segment of the University's local computer network, with no Internet connection established.

4 RESULTS AND DISCUSSION

4.1 *ECDIS backup configuration issues*

The vulnerability scanning of in total six ECDISs was performed, and the summary report on the cyber vulnerabilities detected is shown in Figure 3. The IP address of each of the tested ECDIS (or host by Nessus's terminology) is in the range of 192.168.1.X, with the last octet value of 62, 64, 66, 68, 69 and 70. By comparing mutually scanning summary reports of ECDISs, the number and severity of the detected risky vulnerabilities of each ECDIS are the same. In total, 24 risky vulnerabilities were detected and 34-36 information identified. For each of the tested ECDISs, the report has shown that according to the severity level 1, 7, 15 and 1 vulnerabilities where assigned under the critical, high, medium, and low risk factor, respectively. This, together with the fact that all of the cyber vulnerabilities detected are equal for each of the tested ECDIS (which is analyzed in further detail in Chapters 4.2 and 4.3), indicate the same level of the cyber security of each of the ECDIS.



□	Host	Vulnerabilities
□	192.168.1.62	1 7 15 1 35
□	192.168.1.64	1 7 15 1 35
□	192.168.1.66	1 7 15 1 35
□	192.168.1.68	1 7 15 1 35
□	192.168.1.69	1 7 15 1 34
□	192.168.1.70	1 7 15 1 36

Figure 4. ECDIS vulnerability scanning summary report.

The obtained results can be correlated to the ECDIS backup arrangement, where ECDIS stations with identical ECDIS software performance are required. This implies that most probably the same underlying software and hardware is used for each of the ECDIS stations installations. The identical software and hardware configuration of multiply ECDIS stations leads to the same vulnerability level of each ECDIS to a single cyber threat, resulting in an ideal environment for malicious executive codes distribution via the network for integration or a portable storage device.

4.2 *Underlying operating system vulnerabilities*

The underlying operating system (in our case Microsoft Windows 7) vulnerabilities detected together with descriptions and severity levels are given in Table 2. In total, 8 risky vulnerabilities were detected, from which 1, 1, 5 and 1 with the critical, high, medium, and low severity level, respectively. The critical vulnerability detected is related to the vulnerable version of Server Message Block (SMB) version 1, alerting that immediate installation of a set of security patches released by the vendor is required (Microsoft, 2018). The SMB service vulnerability is particularly interesting for the maritime industry because of one of the most recognized maritime cyber security incident, NotPetya attack on Maersk container shipping company (CERT.be, 2018). NotPetya is a malicious ransomware program that was worldwide rapidly spreading by utilizing vulnerabilities in the SMB v1 protocol (US-CERT, 2018). In the context of the ECDIS backup arrangement, infection of one of the ECDIS stations would most probably result in immediate infection and dysfunctionality of all ECDIS stations in the network.

Table 2. The ECDIS's underlying operating system vulnerabilities detected.

	Service	Vulnerability description	Severity
1	SMB	Remote code execution and information disclosure vulnerabilities exist in Server Message Block version 1 (SMB v1) service.	Critical
2	RDP	Remote code vulnerability exists in the Remote Desktop Protocol (RDP) on the ECDIS.	High
3-5	Terminal Service	Terminal Service running on the ECDIS is vulnerable to a man-in-the-middle attack. Terminal Service running on the ECDIS is vulnerable allowing an attacker to obtain sensitive data. The ECDIS's Terminal Services is not configured to use strong cryptography.	Medium
6	SAM and LSAD	The ECDIS is affected by an elevation of privilege vulnerability in Security Account Manager (SAM) and Local Security Authority (LSAD).	Medium
7	SMB	Signing is not required on the ECDIS's SMB server.	Medium
8	Terminal Service	The ECDIS is affected by the Terminal Service, which is configured to use low encryption level.	Low

The possible preventive solution, in addition to the operating system update and anti-malware software usage, is an adequate setup of the operating system by disabling or blocking the SMB v1 service. It is important to point out that SMB v1 service disabling or blocking may result in obstructing of remote access to shared resources. In the ship environment, this network dysfunctionality is acceptable as ECDIS can and should be operating in the stand-alone configuration. Generally, the underlying operating system updating, as well as adequate setup, could significantly impact the ECDIS software performance, and therefore is to be conducted by the ECDIS equipment manufacturers.

The detected high and medium vulnerabilities are related to omissions of services running on the ECDIS, allowing for possible unauthorized remote code execution and unauthorized remote access gaining. The possible solutions include operating system update by installing a set of security patches and adequate setup by disabling or blocking the vulnerable services (Table 2, services 2-7). The low risk vulnerabilities detected is related to Terminal Service, indicating that low encryption level used, and therefore the recommended action should be taken regarding setup of the operating system service.

4.3 *Third party services vulnerabilities*

The detected vulnerabilities related to the running third party applications on the ECDIS together with descriptions and severity levels are given in Table 3. In total, 16 risky vulnerabilities were detected, from which 6 and 10 with the high and medium severity level, respectively. The detected vulnerabilities rise from active third party services, a web server application (Table 3, vulnerabilities 1-4 and 7-16) and a remote desktop control application (Table 3, vulnerabilities 5-6) that are not required for the expected ship ECDIS performance. The detected vulnerabilities allow for possible ECDIS crashing (denial of service), unauthorized remote code execution, and unauthorized access gaining.

Table 3. Detected vulnerabilities of third party services running on underlying operating system of the ECDIS.

	Service	Vulnerability description	Severity
1-4	Apache web server	Apache web server on the ECDIS is obsolete and no longer maintained by its vendor. Multiple vulnerabilities exist which allow an unauthenticated, remote attacker to cause a denial of service condition, execute code, or obtain sensitive information.	High
5-6	VNC server	Virtual Network Computing (VNC) server installed on the ECDIS allows an attacker to connect as no authentication is required. VNC server installed on ECDIS allows an remote attacker to log into the ECDIS and take a screenshot.	High
7-16	Apache web server	Apache server version is not updated so the ECDIS is vulnerable to: cross-site scripting attacks, arbitrary code executions, the ECDIS crashing, the service stopping, cross-site scripting vulnerabilities, a denial of service, and remote information disclosure.	Medium

The possible solutions are upgraded to a version of the application that is supported by the vendor (Table 3, vulnerability 1), applications update by installing a set of the vendors' security patches, the application's setup by disabling or blocking unnecessary services, and adequate application setup by activating available options. As in the case of the underlying operating system vulnerabilities, the solving activities could also impact the ECDIS performance significantly, and are to be conducted by the ECDIS equipment manufacturers.

4.4 *ECDIS cyber threats analysis*

On the basis of the computational vulnerability scanning conducted, a qualitative cyber threats analysis was performed to identify and estimate cyber threats risk level of ECDIS systems. The identified cyber threats together with estimated impact magnitude and likelihood are given in Table 4. The threats impact has been defined as a magnitude of harm resulting from the successful exploitation of a vulnerability. The impact levels are given as low, medium and high with given values of 10, 50 and 100, respectively. The threats likelihood refers to a probability that a vulnerability is exploited. The likelihood rates are given as high, medium, and low with given values of 1, 0.5, and 0.1, respectively.

Table 4. ECDIS cyber threats identified.

	Threat	Description	Impact	Like-lihood
1	ECDIS backup arrangement	Each ECDIS affected by identical risk, possible immediate total harm	100	0.9
2	Internet connection establishment	Provides remote access for a attacker to the ECDIS.	100	0.1
3	Operating system not updated	Allows exploitation of well known vulnerabilities	100	0.8
4	Operating system unsecure setup	ECDIS performance is reduced and backdoor for intrusions opened	100	0.8
5	Third party applications not updated	Allows exploitation of well known vulnerabilities	90	0.8
6	Third party applications unsecure setup	ECDIS performance is reduced and backdoor for intrusions opened	80	0.8

Four of the six cyber threats identified assigned with the highest impact magnitude (Table 4, threats 1-4) are related to the ECDIS backup arrangement, Internet connection establishment, and underlying operating system updating and adequate setup. The slightly smaller impact is assigned to threats related to the third party applications updating and adequate setup (Table 4, threats 5-6). While the likelihood for most of the threats is assigned to be almost equal, significantly smallest is assigned to the Internet connection establishment.

The cyber risk level is calculated by multiplying the threats' impact magnitude and likelihood rating. The resulting multiplication product indicates the risk level: (i) critical-risk level requiring immediate action (the product is higher then 75), (ii) high-risk level requiring remediation implementation plan (the product is higher then 50), (iii) medium-risk level which may be acceptable over the short period of time (the product is higher then 25), and (iv) acceptable low-risk level. Figure 5 shows radar graph of the results obtained with the qualitative risk analysis.

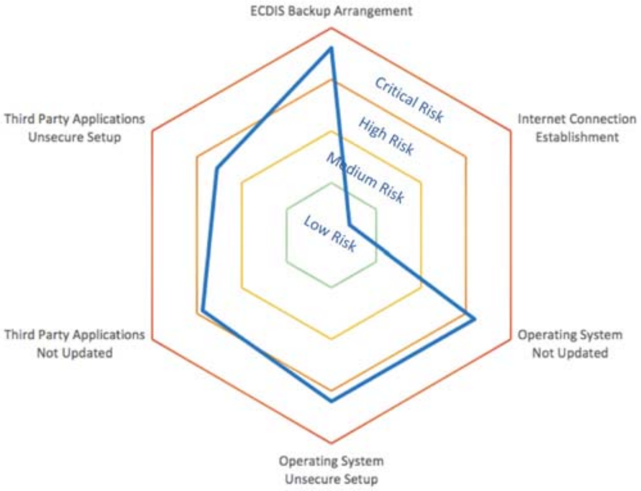


Figure 5. Risk-level radar graph of ECDIS cyber threats identified.

The risk-level radar graph (Figure 5) shows that three cyber threats identified represent the critical-risk level for the ship cyber security. The cyber risk with the highest risk level assigned (the multiplication product of 90) is related to the ECDIS backup arrangement. The identical software and hardware configuration of ECDIS stations represents an ideal environment for malicious executive codes distribution, via the network or portable storage devices (analyzed in detail in Chapter 4.1). The risk levels of threats related to the updating and secure setup of the underlying operating system (analyzed in detail in Chapter 4.2) and active third party applications (analyzed in detail in Chapter 4.3) are assigned as critical and high, respectively. The lowest risk level assigned is related to the Internet connection establishment, with the multiplication product of 10. In the tested environment, Internet connection does not exist, and access of authorized students only is strongly controlled, so the installation of a network device is very unlikely to happen. However, with the Internet connection establishment, all of the cyber threats identified would raise to the highest critical-risk level, requiring immediate action. The results of the risk analysis of the threats identified indicate that while the ECDIS software weaknesses could lead to more serious harm of the ship safe navigation operations (regulated by the IMO performance standards and related circulars), the essential cyber threats actually rise from weaknesses related to the underlying operating system.

5 CONCLUSIONS

The estimation of ECDIS cyber security vulnerabilities that raise from weakness related to the underlying operating system is presented. The cyber vulnerabilities are identified by conducting computational vulnerability scanning using the Nessus Professional software tool. The conducted risk analysis of the cyber threats identified has shown that ECDIS is critically vulnerable to weaknesses raising from the ECDIS backup arrangement and underlying operating system updating and secure setup. In addition, the high risk level is determined for cyber threats from not-updated and insecurely setup third party applications running on the underlying operating system. The results obtained contribute to an understanding of the origin of ECDIS systems cyber security threats. In addition, the presented suggestions for the cyber risks mitigation are applicable to all types of ships critical operational technology computer-based systems.

ACKNOWLEDGEMENTS

The research was financially supported by the University of Rijeka under the research project Cyber Security of Maritime ICT-Based Systems.

REFERENCES

Balduzzi, M., Pasta, A., Wilhoit, K. 2014. A security evaluation of AIS automated identification system. *Proceedings of the 30th Annual Computer Security Applications Conference*, pp 436-445, New Orleans, USA.

Brčić, D., Kos, S., Žuškin, S. 2015. Navigation with ECDIS: Choosing the proper secondary positioning source. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 9: 317- 326.

Burton, J. 2016. Cyber attacks and maritime situational awareness: Evidence from Japan and Taiwan. *Proceedings of the 2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, London, UK.

Federal Cyber Emergency Team (CERT.be). 2018. Petya/NotPetya Malware - Report on worldwide infection. Available at: https://www.cert.be/files/CERTbe_Petya_NotPetya_Malware_E.pdf (10.12.2018).

Filic, M. 2018. Foundations of GNSS Spoofing Detection and Mitigation with Distributed GNSS SDR Receiver. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 12 (4): 649 - 656.

Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., Helkala, K. 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation* 71: 1025- 1039.

Hassani, V., Crasta, N., Pascoal, A.M. 2017. Cyber security issues in navigation systems of marine vessels from a control perspective. *Proceedings of the International Conference on Ocean, Offshore Mechanics and Arctic Engineering*, Trondheim, Norway.

International Hydrographic Organization (IHO) (2017). *Information on IHO Standards related to ENC and ECDIS. Version 1.1.* Monaco: IHO.

International Hydrographic Organization (IHO) (2018). *Current IHO ECDIS and ENC Standards*. Monaco: IHO.

International Maritime Organization (2006). *MSC.232(82): Adoption of the revised performance standards for Electronic Chart Display and Information Systems (ECDIS)*. London: IMO.

International Maritime Organization (2009). *MSC.282(86): Adoption of amendments to the International Convention for the Safety Of Life At Sea, 1974. Annex 1.* London: IMO.

International Maritime Organization. (2010). *SN.1/Circ.266/Rev.1: Maintenance of Electronic Chart Display and Information System (ECDIS) software.* London: IMO.

International Maritime Organization (2014). *International Convention for the Safety of Life at Sea (SOLAS), 1974 as amended.* London: IMO.

International Maritime Organization. 2017. Resolution MSC.1/Circ.1503/Rev.1, ECDIS – GUIDANCE FOR GOOD PRACTICE. London: IMO.

International Maritime Organization. 2017. Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems. London: IMO.

International Maritime Organization. 2017. Resolution MSC-FAL.1/Circ.3, Guidelines On Maritime Cyber Risk Management. London: IMO.

Kessler, G.C., Craiger, J.P., Haass, J.C. 2018. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3): 429 - 437.

Lee, Y.C., Park, S.K., Lee, W.K., Kang, J. 2017. Improving cyber security awareness in maritime transport: A way forward. *Journal of the Korean Society of Marine Engineering*, 41: 738-745.

Microsoft. 2018. Microsoft Security Bulletin MS17-010 - Critical. Available at: https://technet.microsoft.com/library/security/MS17-010 (10.12.2018).

Nessus. 2018. Tenable Products: Nessus Professional version 8. Available at: https://www.tenable.com/products/nessus/nessus-professional (10.12.2018).

Polatid, N., Pavlidis, M., Mouratidis, H. 2018. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards Interfaces* 59, 74– 82.

Shapiro, L.R., Maras, M.H., Velotti, L., Pickman, S., Wei, H.L., Till, R. 2018. Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security* 8, 1–19.

Svilicic, B., Kamahara, J., Rooks, M., Yano, Y. 2019. Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*: in press. Available at: https://doi.org/10.1017/S0373463318001157 (25.02.2019).

Svilicic, B., Celic, J., Kamahara, J., Bolmsten, J. 2018. A Framework for Cyber Security Risk Assessment of Ships. *Proceedings of 19th International Association of Maritime Universities Conference*, pp 21-28, Barcelona, Spain.

Svilicic, B., Kras, A. 2005. Computer Systems Privacy Protection. *Pomorstvo - Scientific Journal of Maritime Research* 19 (1), 275–284.

Tam, K., Jones, K. 2019. MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*: in press. Available at: https://doi.org/10.1007/s13437-019-00162-2 (25.02.2019).

Transas. 2018. Navi-Sailor 4000 ECDIS. Available at: http://www.transas.com/products/navigation/ecdis/ECDIS(10.12.2018).

United States Computer Emergency Readiness Team (US-CERT). 2018. Alert (TA17-181A) Petya Ransomware. Available at: https://www.us-cert.gov/ncas/alerts/TA17-181A (10.12.2018).