THE JOURNAL OF NAVIGATION (2019), **72**, 1108–1120. © The Royal Institute of Navigation 2019
doi:10.1017/S0373463318001157

Maritime Cyber Risk Management: An Experimental Ship Assessment

Boris Svilicic[1], Junzo Kamahara[2], Matthew Rooks[2] and Yoshiji Yano[2]

[1](*University of Rijeka, Faculty of Maritime Studies, Studentska ulica 2, 51000 Rijeka, Croatia*)
[2](*Kobe University, Graduate School of Maritime Sciences, 5-1-1 Fukaeminami-machi, Higashinada-ku, Kobe, Japan*)
(E-mail: svilicic@pfri.hr)

The maritime transport industry is increasingly reliant on computing and communication technologies, and the need for cyber risk management of critical systems and assets on vessels is becoming critically important. In this paper, a comprehensive cyber risk assessment of a ship is presented. An experimental process consisting of assessment preparation activities, assessment conduct and results communication has been developed. The assessment conduct relies on a survey developed and performed by interviewing a ship's crew. Computational vulnerability scanning of the ship's Electronic Chart Display and Information System (ECDIS) is introduced as a specific part of this cyber security assessment. The assessment process presented has been experimentally tested by evaluating the cyber security level of Kobe University's training ship *Fukae-maru*. For computational vulnerability scanning, an industry-leading software tool has been used, and a quantitative cyber risk analysis has been conducted to evaluate cyber risks on the ship.

KEYWORDS

1. Maritime cyber security. 2. Computational vulnerability scanning. 3. Quantitative risk analysis.

Submitted: 1 November 2018. Accepted: 26 December 2018. First published online: 7 February 2019.

1. INTRODUCTION.

Ships are increasingly using information and operational technology systems that depend on digitisation, networking and integration. As the reliance on computing and communication technologies is growing, the need for cyber risk management is becoming critically important (Polatid et al. 2018; Hareide et al., 2018; Shapiro et al., 2018; Botunac and Gržan, 2017; Lee et al., 2017; Hassani et al., 2017; Burton, 2016; Balduzzi et al., 2014; Svilicic and Kras, 2005). Recently, the International Maritime Organization (IMO) has published Guidelines on high-level recommendations for maritime cyber risk management (IMO MSC, 2017c). While maritime regulations and policies currently do not adequately govern cyber security in the same way as other aspects of ship security and safety, cyber security risk assessment can be considered as being partly regulated by the International Ship and Port Facility Security (ISPS) Code established by the IMO (IMO, 2013). However, the IMO has decided to incorporate cyber risk management

المنارة للاستشارات
www.

Figure 1. Training ship *Fukae-maru*.

into the International Safety Management (ISM) Code safety management system on ships by 1 January 2021 (IMO MSC, 2017b).

Systematic assessment of maritime cyber risk management is essential for improving cyber security on ships. Ship cyber risk assessment represents a complex set of interdependent and intersecting actions that act as safeguards against the challenges presented by recent innovations in computing and communication technologies and key shipboard operations. An effective ship cyber risk assessment should provide a method to balance appropriate cyber safeguard mechanisms and measures of evaluating a ship's critical cyber systems and assets, key shipboard operations, existing safeguard controls, assessed cyber threats and vulnerabilities, and a determined risk level.

In this paper, a comprehensive cyber risk assessment of a ship is presented to offer guidance for improving the security level of cyber systems on board ships. The assessment was conducted on the training ship *Fukae-maru* (shown in Figure 1) (Kobe University, 2018), and was based on a combination of a survey given to the ship's crew and computational vulnerability scanning of the ship's Electronic Chart Display and Information System (ECDIS). The ship's cyber security level has been evaluated by a quantitative cyber risk analysis.

2. CYBER SECURITY ASSESSMENT PROCESS.

The cyber security assessment of the training ship *Fukae-maru* was conducted according to the assessment process shown in Figure 2. The developed assessment process relies on published guidelines and practices (IMO MSC, 2017c; NIST, 2018, BIMCO, 2017; DNV-GL, 2016). The process consists of three main phases: assessment preparation, conduct and results communication. The process is not intended for initial assessment only, but also for periodic implementation to respond to rapid technological changes in a ship environment.

المنارة للاستشارات
www.

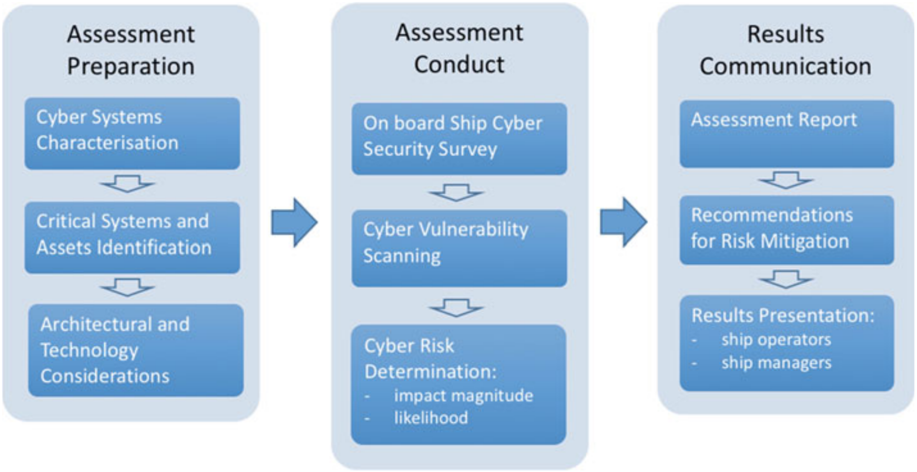
Assessment Preparation
Cyber Systems Characterisation
Critical Systems and Assets Identification
Architectural and Technology Considerations
Assessment Conduct
On board Ship Cyber Security Survey
Cyber Vulnerability Scanning
Cyber Risk Determination:
- impact magnitude
- likelihood
Results Communication
Assessment Report
Recommendations for Risk Mitigation
Results Presentation:
- ship operators
- ship managers

Figure 2. Cyber security assessment process conducted.

Table 1. *Fukae-maru's* ECDIS system technical specification.

ECDIS	Manufacturer	Japan Radio Co. Ltd.
	Model	JAN-901B
	Serial No.	KG 01130
	USCG ID	165.123/10/0
	IMO compliant	Yes
General	Operating system	Windows XP embedded
	Power supply	AC 100-115, 200-230 V ±10%, 60/50 Hz ±5%
Chart management	Updating	Semi-auto/manual
	Data correction	Available
Interfaces	Gyro input	IEC61162-2
	Log input	IEC61162-1
	Remote maintenance	Possible
	Copying route	FD/USB
	Network	LAN (10/100 Mbps)
Hardware design	Vibration absorber	Yes
	CD/DVD ROM drive	Yes
	Dual hard disk	Yes
	Silicon disk	Yes
	Battery for auto shut down	Yes
	Network adapter (LAN)	Yes
	Serial interface	Gyro, Doppler log, GPS, NAVTEX, Echo sounder, ARPA, AIS and Auto pilot

In the first phase of the conducted assessment, the ship cyber systems were characterised by gathering information about general ship technical specifications. The identification of critical ship systems and assets was conducted on the basis of the ship's technical specification documentation and implemented together with the following architectural and technological considerations. Table 1 shows the technical specifications of the ship's ECDIS system, which is analysed in further detail in Chapter 3.

المنارة للاستشارات
www.

The first phase outputs were used to develop a survey for on board ship estimation of cyber security safeguards implemented on the ship (second phase of the process). Compared to other types of ship assessment (Ernstsen and Nazir, 2018), the most specific element of the cyber security risk assessment is the conduct of computational vulnerability scanning of the ship's critical cyber systems. Computational cyber vulnerability scanning is a process of reviewing critical systems and assets to locate and identify known weaknesses. In the last segment of the assessment conduct phase, the cyber risk is determined on the basis of likelihood and impact magnitude of the threats and vulnerabilities detected by the survey and vulnerability scanning report. In the final phase of the process, the assessment results are reported, a recommendation for cyber risk mitigation is developed, and overall assessment results are presented to the ship's crew.

3. ON BOARD SHIP CYBER SECURITY SURVEY.

The goal of performing and documenting the ship cyber security survey is to identify non-existing and/or insufficient safeguard mechanisms and measures. In addition, the cyber security survey is essential to confirm that cyber security safeguard mechanisms and measures are in place on the ship. To collect the relevant information, we developed a questionnaire on the basis of the ship cyber risk critical systems and assets identified. The form used for the survey conducted by interviewing the ship crew is given in Table 2.

The survey is segmented into four parts regarding the ship's cyber critical systems: the cyber security management system, bridge systems, power systems and networking systems (Table 2). Each of the segments has been individually categorised regarding the related assets and possible cyber threats. Data collection was conducted by interviewing the ship's crew, the ship's captain and the first officer for the cyber security management system, bridge systems, and networking systems. The first engineer officer was interviewed for the power systems. The evaluation results from these surveys concerning cyber security safeguard mechanisms and measures are shown in Table 3.

In Table 3, the critical network security system (see Table 2) is incorporated in the bridge systems and power systems. The survey results indicate that cyber security is integrated in the ship policies and procedures only in part, and policies and procedures mainly dedicated to cyber security are not fully developed. However, the policies and procedures are well communicated and periodically reviewed. The ship's crew is trained by the ship's systems vendors, as well as by the University. The bridge systems and power systems demonstrated an equal level of cyber security. On the vessel itself, an Internet connection is not established, a physical access policy is in place, the handling of portable devices is controlled, logical authentication is in place, authorisation using strong control mechanisms is enforced and confidential agreements with all suppliers and sub-suppliers are in place.

4. CYBER VULNERABILITY COMPUTATIONAL SCANNING.

Computational cyber vulnerability scanning is a process of reviewing critical systems and assets to locate and identify known weaknesses. The computational scanning of the ship's ECDIS system was performed using an industrial-leading software tool, Nessus Professional (Nessus, 2018). As the ECDIS operates in the stand-alone configuration with no Internet connection, a laptop with the vulnerability scanner pre-installed was directly connected to the ECDIS

المنارة للاستشارات
www.

Table 2. Form used for conducting the survey by interviewing the ship crew.

Critical System	Assets	What are the threats?	Protection safeguards	Risk Evaluation	
				Impact	Likelihood
Cyber security management system	Policies and procedures	Policies and procedures Communication to crew Periodical review Confidential agreements Regular audits			
	Training and awareness	Program is developed Program is conducted			
Bridge system	ECDIS	Authentication and access controls Audit and logs Software security Communication security Physical and environmental protection			
Power systems	Power management	Authentication and access control Audit and logs Software security Communication security Physical and environmental protection			
Network security	Security software installed	Anti-virus software Firewall Intrusion detection system Communication security Logging and monitoring			

via an Ethernet cross cable. While the ECDIS application was running under administrative credentials, the remote vulnerability scanning was performed without administrative privileges. The testing setup is shown in Figure 3.

The scanning report summary including the ECDIS IP address (192·168·60·59) is shown in Figure 4. The computational scanning resulted in 14 vulnerabilities detected and 23 information packages identified. Half of the vulnerabilities detected have been assigned designations under the critical risk factor, indicating the need for urgent action in solving security issues. From the rest of the vulnerabilities, two, four and one have been respectively marked with high, medium and low risk factors, respectively.

The ECDIS critical cyber vulnerabilities detected together with descriptions and possible solutions are given in Table 4. The detected critical cyber vulnerabilities (Table 5, vulnerabilities 1 and 2) alert that the ECDIS system (which is IMO compliant) is implemented on a computer with a version of the operating system (Microsoft Windows XP, Service Pack 2) that is has not been supported by the vendor for more than four years (Microsoft, 2018). The lack of support implies that no new security patches for the operating system have been released by the vendor. In addition, the vendor is unlikely to investigate or acknowledge reports of newly discovered vulnerabilities. This allows an attacker to exploit well-known vulnerabilities using widely available tutorials, for which

المنارة للاستشارات
www.

Table 3. Cyber security measures and mechanisms incorporated.

Critical System	Measure/Mechanism	Description
Cyber security management system	Policies and procedures	Policies and procedures partially related to cyber security are developed Policies and procedures are communicated to the all crew Policies and procedures are periodically reviewed
	Incident handling	All cyber security incidents are reported Incident handling procedures are in place
	Training and awareness	Training and awareness program for the ship crew Provided by a device/system manufacture
Bridge systems	Internet communication	Connection to the Internet is not established
	Access controls	Access control policy is in place Physical access is provided to authorized personnel only Handling of portable devices is controlled
	Authentication controls	Authentication policy is in place All control mechanisms are enforced Procedure for authorized access Log-out obligation is enforced All default passwords have been changed
	Confidential agreements	Confidential agreement is in place for all sub-suppliers
Machinery management and power control systems	Internet communication	Connection to the Internet is not established
	Access controls	Access control policy is in place Physical access is provided to authorized personnel only Handling of portable devices is controlled
	Authentication controls	Authentication policy is in place All control mechanisms are enforced Procedure for authorized access Log-out obligation is enforced All default passwords have been changed
	Confidential agreements	Confidential agreement is in place for all sub-suppliers

significant expertise and knowledge in computational technologies is not needed. As a consequence of the outdated operating system, five critical vulnerabilities related to different active services were raised and detected by the vulnerability scanner (Table 4, vulnerabilities 3 - 7). The common characteristic of these vulnerabilities is a provision of remote access to the ECDIS with logically authorised privileges. The possible solution for these detected critical vulnerabilities is to upgrade to a supported version of the operating system with a supported service pack and appropriate security patch. It is important to point out that the supporting operating system updates could significantly impact the ECDIS software performance (IMO MSC, 2017a), and therefore it should be conducted by the ECDIS equipment manufacturer.

المنارة للاستشارات
www.

Table 4. ECDIS cyber vulnerabilities computationally detected and assigned with the critical risk factor.

	Vulnerability	Description	Risk Factor	Possible Solution*
1.	MS Windows XP unsupported	Support for this operating system by the vendor (Microsoft) ended 8 April 2014. Lack of support implies that no new security patches for the product are released by the vendor. In addition, the vendor is unlikely to investigate or acknowledge reports of vulnerabilities.	Critical	Upgrade to a version of operating system that is currently supported
2.	Unsupported Windows operating system	The version of operating system is missing a service pack. As a result, it is likely to contain security vulnerabilities.	Critical	Upgrade to a supported service pack
3.	Vulnerability in SMB could allow remote code execution	The version of the operating system contains a flaw in the Server Message Block (SMB) service implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.	Critical	Vendor has released a set of patches for the operating system.
4.	Vulnerability in Server service could allow remote code execution	The ECDIS is vulnerable to a buffer overrun in the Server service that may allow an attacker to execute arbitrary code on the ECDIS with ultimate privileges.	Critical	Vendor has released a set of patches for the operating system.
5.	Server service crafted Remote Procedure Call (RPC) request handling remote code execution	The ECDIS is affected by a remote code execution vulnerability in the Server service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with ultimate privileges.	Critical	Vendor has released a set of patches for the operating system.
6.	SMB vulnerabilities remote code execution	The ECDIS is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the ECDIS.	Critical	Vendor has released a set of patches for the operating system.
7.	Security update for SMB service	The ECDIS is affected by multiple vulnerabilities: • Multiple remote code execution vulnerabilities exist in SMBv1 service. An unauthenticated, remote attacker can exploit these vulnerabilities to execute arbitrary code. • An information disclosure vulnerability exists in SMBv1 service. An unauthenticated, remote attacker can exploit this to disclose sensitive information.	Critical	Vendor has released a set of patches for the operating system.

*Implementation of the possible solution is to be conducted by the ECDIS equipment manufacturer.

المنارة للاستشارات
www.manaraa.com

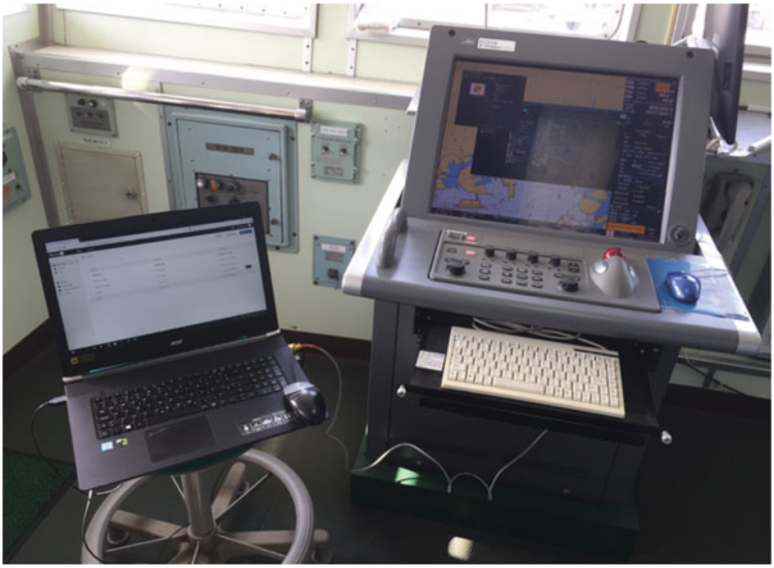

Figure 3. Testing setup for computational vulnerability scanning of ECDIS.

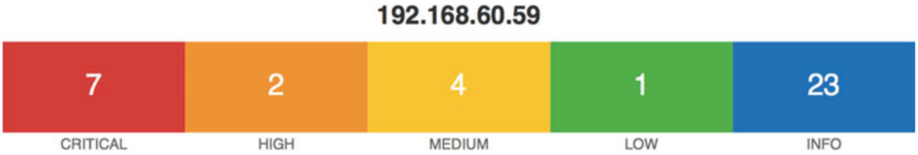

Figure 4. Nessus Profession vulnerability scanner summary report on vulnerabilities detected.

Table 5 shows detected vulnerabilities classified with risk factors of high, medium and low. The detected high-risk factor vulnerabilities are related to omissions of services running on the ECDIS, allowing for possible unauthorised remote code execution. The solution requires urgent installation of a set of security patches for the operating system provided by the vendor. The medium and low risk factor vulnerabilities detected are also related to the remote establishment of unauthorised access. The possible solution for these vulnerabilities includes adequate configuration of the operating system by activating available options. It is worth noting that the detected vulnerabilities arise from services running on the ECDIS that are not required for the expected functionality of the ECDIS operating in the stand-alone configuration, as it is on the *Fukae-maru*. With an adequate operating system setup, which should be based on the disabling of unnecessary services, the cyber security level of the ECDIS would be significantly improved without influencing fundamental functionality. As in the case of the supporting operating system updates, these activities could also impact the ECDIS software performance significantly and are to be conducted by the ECDIS equipment manufacturer.

5. CYBER RISK DETERMINATION. On the basis of the survey conducted and computational vulnerability scanning results, a cyber risk analysis was performed to identify and categorise cyber threats to which the ship is exposed. Table 6 shows the cyber threats

المنارة للاستشارات
www.

Table 5. ECDIS cyber vulnerabilities computationally detected.

	Vulnerability	Description	Risk Factor	Possible Solution*
1.	Server service could allow remote code execution	The ECDIS is vulnerable to heap overflow in the Server service that may allow an attacker to execute arbitrary code on the remote host with ultimate privileges. The ECDIS is also affected by an information disclosure vulnerability in SMB service that may allow an attacker to obtain portions of the memory of the ECDIS.	High	Vendor has released a set of patches for the operating system.
2.	Remote Desktop service could allow remote code execution	An arbitrary remote code vulnerability exists in the implementation of the RDP service running on the ECDIS. An unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code.	High	Vendor has released a set of patches for the operating system.
3.	SMB NULL session authentication	The ECDIS is running a Microsoft Windows operating system. It is possible to log into it using a NULL session (i.e., with no login or password).	Medium	Secure configuration of the operating system is required.
4.	SMB signing disabled	Signing is not required on the SMB service running on the ECDIS. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the ECDIS.	Medium	Secure configuration of the operating system is required.
5.	Terminal Services service encryption level is medium or low	The Terminal Services service running on the ECDIS is not configured to use strong cryptography. An attacker could eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.	Medium	Secure configuration of the operating system is required.
6.	Remote Desktop Protocol service man-in-the-middle weakness	The RDP service running on the ECDIS is vulnerable to a man-in-the-middle attack. An unauthenticated, remote attacker could obtain any sensitive information transmitted, including authentication credentials.	Medium	Secure configuration of the operating system is required.
7.	Terminal Services service encryption level is not FIPS-140 compliant	The Terminal Services service running on the ECDIS is not configured to use RDP encryption level of FIPS-140 compliance.	Low	Secure configuration of the operating system is required.

*Implementation of the possible solution is to be conducted by the ECDIS equipment manufacturer

المنارة للاستشارات
www.manaraa.com

Table 6. Cyber threats determined.

Threat	Description	Critical System/Asset	Likelihood	Impact Magnitude
1. Physical access	Provides physical access for a attacker to targeted ships critical system/asset	Bridge systems/ECDIS Machinery management and power control systems	0·2	100
2. Operating system support and security patches	Allows exploitation of well known vulnerabilities (no need for significant expertise and knowledge in computing)	Bridge systems/ECDIS Machinery management and power control systems	0·2	90
3. Operating system configuration	Unnecessary services activated reduces performance and opens backdoor for intrusions	Bridge systems/ECDIS Machinery management and power control systems	0·2	80
4. Internet connection establishment	Provides access for an attacker to target a ship critical system/asset	Bridge systems/ECDIS Machinery management and power control systems	0·1	100
5. Authorised access	Provides logical access for an attacker to target a ship critical system/asset	Bridge systems/ECDIS Machinery management and power control systems	0·1	80
6. Awareness	Crew is not familiar with cyber security policies, procedures and agreements, and practice insufficient cyber hygiene	All critical systems/ assets	0·5	15
7. Polices and procedures	Roles and responsibilities are not clearly defined	All critical systems/ assets	0·5	10
8. Training	Crew is not adequately trained to perform their cyber security related duties and responsibilities	All critical systems/ assets	0·5	10
9. Continuous evaluation and improvement	Periodic evaluation and improvement are required to respond to rapid technological changes	All critical systems/ assets	0·2	10

determined together with estimated likelihood and impact magnitude of their exposure. The threat likelihood has been defined as a rating of the probability that a vulnerability is exploited. The likelihood levels are given as low, medium and high with given values of 0·1, 0·5 and 1, respectively. The impact refers to the magnitude of harm resulting from

المنـــارة للاستشارات
www.

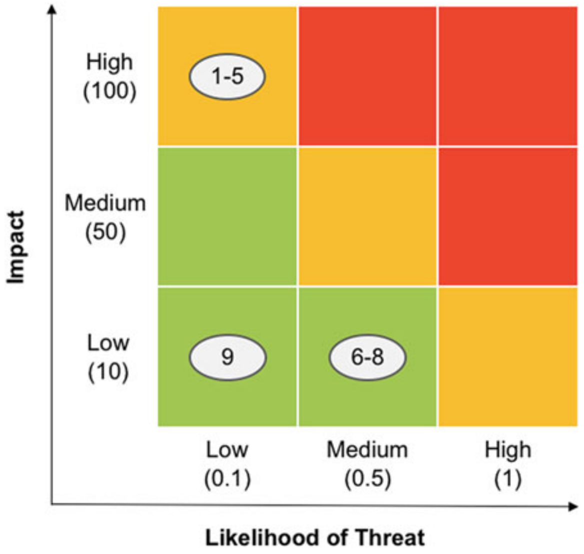

Figure 5. Risk-level matrix with qualitative risk analysis of cyber threats determined.

successful exploitation of a vulnerability. The impact magnitude rates are given as high, medium, and low with given values of 100, 50 and 10, respectively.

Five of the nine cyber threats determined (Table 6) are related to the bridge systems and power systems, while four of the remaining threats influence all of the ship cyber critical systems. On the basis of the evaluated impact magnitude and likelihood of the threats determined, a qualitative risk analysis was performed. Cyber risk level is calculated by multiplying the threat likelihood ratings with the impact magnitude of the vulnerability exploited. The result indicates qualitative risk levels: (i) critical-risk level requiring immediate action (multiplication product higher then 90), (ii) high-risk level requiring remediation implementation plan (multiplication product higher then 50), (iii) medium-risk level which may be acceptable over the short term (multiplication product higher then 10), and (iv) acceptable low-risk level (multiplication product lower then 10). Results of the qualitative risk analysis of cyber threats determined are given in the cyber risk-level matrix in Figure 5.

The risk-level matrix (Figure 5) indicates that the first five cyber threats determined (see Table 6) represent the medium-risk level for ship cyber security. The cyber risk with the highest risk level assigned (medium-risk level with the multiplication product of 20) is related to physical access. While safety procedures in the maritime field are traditionally focused on physical security, for a ship's electronic equipment, the establishment of unauthorised physical access represents a threat with the highest impact magnitude. An example frequently performed on a ship is plugging a malware-infected Universal Serial Bus (USB) memory stick into ECDIS for the purpose of an electronic charts update. In addition to raising awareness on the cyber hygiene and anti-malware tools usage, the ECDIS hardware (including USB ports) should be kept in a locked case to prevent physical access by unauthorised personnel. However, for a training ship with strongly controlled student access, the threat likelihood is estimated as low (value of 0·2, see Table 5). The four medium-risk level cyber threats determined are related to the operating system maintenance and

المنارة للاستشارات
www.

remote authorised access (threats 2-5 in Table 5). As the assessment has been conducted on a training ship with no Internet connection, the medium-risk level risks are acceptable over the short term, at least until an Internet connection is established on the ship. With an active Internet connection, the cyber risks would rise to the critical-risk level, requiring immediate action. The acceptable low-risk level has been assigned to the cyber risks affecting all the ship critical systems (threats 6-9 in Table 5) and requiring the development of cyber security-focused policies and procedures, crew training, awareness raising and periodic evaluation and improvements. While the low-risk level cyber risks do not necessarily have to be solved in the short term, the recommended action should be taken to mitigate the cyber risks.

6. CONCLUSIONS. A comprehensive experimental assessment of the *Fukae-maru's* cyber security management has been presented. An assessment process consisting of three phases was developed: the assessment preparation activities, assessment conduct and results communication. The ship's incorporated cyber security safeguard measures and mechanisms were identified via the developed survey and by interviewing the ship's crew. Computational vulnerability scanning of the ship's ECDIS system has been introduced as a specific part of cyber security assessment conduct and the Nessus Professional software tool was used for this. A quantitative cyber risk analysis has been conducted for evaluation of the ship cyber risks. The presented assessment process is comprehensive and applicable to all ships, offering guidelines for mitigating cyber risks and to improve the cyber security level of ship cyber critical systems and assets.

FINANCIAL SUPPORT

The research was financially supported by the Erasmus+ programme of the European Union (grant number 2016-1-HR01-KA107-021738) and the Faculty of Maritime Studies University of Rijeka under the research project Internet of Maritime Things and Cyber Security.

REFERENCES

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

Baltic and International Maritime Council. (BIMCO). (2017). The guidelines on cyber security onboard ships. Version 2.0. BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

Botunac, I. and Gržan, M. (2017). Analysis of software threats to the automatic identification system. *Brodogradnja*, **68**, 97–105.

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.

Det Norte Veritas – Germanischer Lloyd (DNV-GL). (2016). Cyber security resilience management for ships and mobile offshore units in operation. DNVGL-RP-0496. DNV-GL.

Ernstsen, J. and Nazir, S. (2018). Consistency in the development of performance assessment methods in the maritime domain. *WMU Journal of Maritime Affairs*, **17**, 71–90.

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

Hassani, V., Crasta, N. and 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.

المنارة للاستشارات
www.

International Maritime Organization - Maritime Safety Committee (IMO-MSC). (2017a). ECDIS – Guidance for good practice. MSC.1/Circ.1503/Rev.1. International Maritime Organization.

IMO-MSC. (2017b). Maritime Cyber Risk Management in Safety Management Systems. MSC 98/23/Add.1. International Maritime Organization.

International Maritime Organization (IMO). (2013). International Ship and Port Facility Security (ISPS) Code. SOLAS/CONF.5/34. International Maritime Organization.

IMO. (2017c). Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3. International Maritime Organization.

Kobe University. (2018). Research Facilities: The training ship Fukae-maru. Available: https://www.maritime.kobe-u.ac.jp/en/study/fukaemaru_e.html.

Lee, Y.C., Park, S.K., Lee, W.K. and 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: Search product lifecycle. Available: https://support.microsoft.com/en-us/lifecycle.

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology.

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

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

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

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

المنارة للاستشارات

www.

Copyright © The Royal Institute of Navigation 2019

www.