THE JOURNAL OF NAVIGATION (2020), **73**, 547–558.
doi:10.1017/S0373463319000808

Towards a Cyber Secure Shipboard Radar

Boris Svilicic, Igor Rudan, Vlado Frančić and Djani Mohović

(*University of Rijeka, Faculty of Maritime Studies, Studentska ulica 2, 51000 Rijeka, Croatia*)
(E-mail: svilicic@pfri.hr)

This paper presents a comparative cyber security resilience estimation of shipboard radars that are implemented on two oil/chemical tankers certified as SOLAS ships. The estimated radars were chosen from the same manufacturer, but belonged to different generations. The estimation was conducted by means of ships' crew interviews and computational testing of the radars using a widely deployed vulnerability scanning software tool. The identified cyber threats were analysed qualitatively in order to gain a holistic understanding of cyber risks threatening shipboard radar systems. The results obtained experimentally indicate that potential cyber threats mainly relate to maintenance of the radars' underlying operating system, suggesting the need for regulatory standardisation of periodic cyber security testing of radar systems.

KEYWORDS

1. Navigation Safety. 2. Radar. 3. Maritime Cyber Security. 4. Vulnerability Scanning.

Submitted: 17 April 2019. Accepted: 17 August 2019. First published online: 7 November 2019.

1. INTRODUCTION. Shipboard radar equipment has been a major aid to navigation for the past seven decades, helping the officer on duty to carry out a safe navigational watch. Over the years, as radar technology has developed, it has become a mandatory navigation tool required on any ship of 300 GT and above, used for the identification, tracking and positioning of vessels in order to enhance collision avoidance and safely navigate a ship. Remarkable advances in computer technology over the last two decades have also influenced radar development, resulting in complex software-based systems. With the increasing reliance on digitalisation, software development and network integration – not only of radar but other shipboard navigational equipment – the need to safeguard shipping from cyber threats has acquired great importance (Lee et al., 2017; Fernández-Hernández et al., 2018; Hareide et al., 2018; Lewis et al., 2018; Polatid et al., 2018; Shapiro et al., 2018; Svilicic et al., 2019; Tam and Jones, 2019).

The International Maritime Organization (IMO) recently issued *Guidelines on Maritime Cyber Risk Management* (IMO, 2017a), amended to include cyber security risk management in safety management systems starting from 1 January 2021 (IMO, 2017b). The aforementioned requirement encourages maritime administrations to ensure that cyber security risks are appropriately addressed in safety management systems, and that cyber

Figure 1. Oil/chemical tankers on-board of which cyber security estimation was conducted.

security risk management, as part of the safety management system, follows the objectives and functional requirements of the International Safety Management Code. On the other hand, functionality of the radar software is standardised by IMO through their performance standards for radar equipment (IMO, 2004). However, the supporting hardware and the underlying operating system required for running the radar software is determined by radar equipment manufacturers.

Recently, we presented an experimental cyber risk assessment of a shipboard Electronic Chart Display and Information System (ECDIS) based on the vulnerability scanning approach (Svilicic et al., 2019). In this paper, a comparative cyber security resilience estimation of shipboard radars implemented on two oil/chemical tankers (see Figure 1) is presented. In order to study the source of cyber security risks in shipboard radar systems and gain a holistic understanding of them, two radars from the same manufacturer but belonging to different generations were estimated. The estimation process was adjusted to the ships' type and the radars' technical characteristics, and conducted by means of a ships' crew interview and a radar systems vulnerability scan using a widely deployed software tool. The radars' cyber threat risk levels, which were determined qualitatively, were compared, and mitigation solutions are discussed.

2. ESTIMATION PROCESS.

The estimation of the shipboard radars' cyber security resilience was conducted on two oil/chemical tankers certified as SOLAS ships, mainly engaged in coastal navigation. The estimation process was developed on the basis of the published guidelines and practices (DNV-GL, 2016; BIMCO, 2017; IMO 2017a; NIST, 2018), and it consisted of four major phases: preparation, conducting, risk level determination and results communication. The process flow is shown on Figure 2.

In the preparation phase, a survey for the identification of the implemented cyber security safeguards was developed on the basis of a characterisation of the ships' radar systems by referring to the ships' and radars' technical documentation (see Section 4 for details). The second phase started with the ships' crew interview using the questionnaire developed, and it continued with the vulnerability scan of the radars (see Section 5 for details). Based on the results obtained, a risk level determination of the cyber threats that were identified was conducted (see Section 6 for details). In the final phase, the estimation results, together with cyber risk mitigation recommendations, were reported to the ships' crew and managers.

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

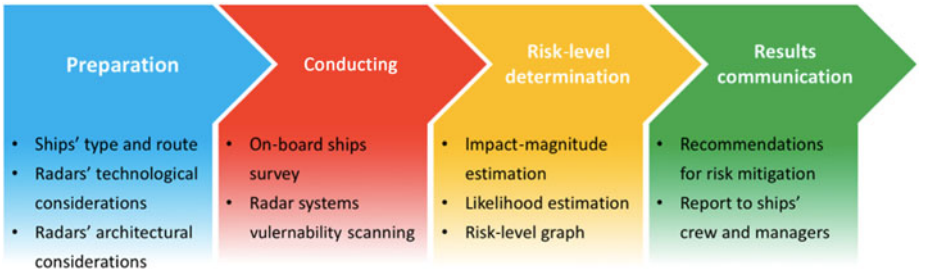

Figure 2. The radars' cyber security estimation process flow.

Table 1. The shipboard radars' specifications.

		Radar #1	Radar #2
General	Manufacturer	Japan Radio Company Ltd.	Japan Radio Company Ltd.
	Model	Alphascan 5925-6X	JMA-9922-6XA
	IMO compliant	Yes	Yes
	Approved type	BABT-MED000107	RAAS4NM9-25kpon-35
	Approval date	November 2016	December 2003
	Installation date	2018	2005
Interfaces	Serial NMEA	IEC 61162-1	IEC 61162-1
	Serial high speed	IEC 61162-2	-
	Ethernet interface	IEC 61162-450	Ethernet (10 Mbps)
	Remote media	USB	USB
	Remote maintenance	Possible	-

3. THE SHIPBOARD RADARS. The estimated radars are from the same manufacturer, the Japan Radio Company Ltd. However, two different models were estimated: Alphascan 5925-6X (named Radar #1) and JMA-9922-6XA (named Radar #2). The radars' technical specifications are given in Table 1.

The radars are IMO compliant and their software meets IMO performance standards. Radar #1 approval dates from 2016 and that of Radar #2 is from 2003. Radar #1 was installed on the ship in 2018, and Radar #2 in 2005. The radars are implemented in a stand-alone configuration. Although an active Ethernet network adapter is incorporated in each of the radars, the sensors' data are gathered via a serial interface. The sensors integrated include a Global Positioning System, heading gyrocompass, speed log, Automatic Identification System and radar scanner.

4. ON-BOARD SHIP SURVEY. The on-board ship survey was conducted to identify the existing protection measures and mechanisms, but also to identify missing or weak safeguards. On the basis of the radars' technological and architectural characteristics, a questionnaire for collecting the relevant information was developed. The form used while interviewing the ships' crew focused on four critical ship assets: security policies and procedures, crew training and awareness, the radar, and the integration network (see Table 2).

The identified protection measures and mechanisms implemented on the ships are shown in Table 3. The survey outcomes related to the cyber security management showed that

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

Table 2. The form used for interviewing the ships' crew.

Critical asset	Threats	Safeguards implemented	Threat evaluation	
			Impact	Likelihood
Security policies and procedures	Cyber-related roles and responsibilities do not exist			
	Insufficient communication with the crew			
	Procedures for incident handling do not exist			
	Periodical reviews are not conducted			
	Periodical audits are not conducted			
Training and awareness	The crew is not familiar with the radar operating procedures			
	Lack of crew awareness and insufficient cyber hygiene			
Radar	Access controls do not exist			
	Physical protection controls do not exist			
	Remote authentication controls do not exist			
	Audit log activities are not recorded and kept			
	Incident handling procedures do not exist			
	Internet connection exists			
Integration network	Malicious code protections do not exist			
	Network privacy safeguards do not exist			
	Software updates are not implemented			
	Monitoring of security activities do not exist			

security policies and procedures were implemented, well communicated with the crew, and periodically reviewed and audited. However, policies and procedures that are fully dedicated to cyber security have not been developed. The training of the ships' crew was conducted by the radar vendor, cyber security awareness was at a high level and the crew practised sufficient cyber hygiene. Strong physical access controls were implemented, access was allowed only to authorised personnel and all hardware interfaces were stored in a locked case. Confidentiality agreements were signed with the radar vendor. A network connection was not established on either of the radars.

The protection mechanism implemented that differs between the radars is the cyber security software. The protection is related to the radar software underlying the hardware and operating system, and was implemented only on Radar #1. Radar #1 belongs to the new generation of radar equipment, the operating system features and hardware resources of which allow implementation of this protection. This is discussed in further detail in the following sections. However, it is important to emphasise that the existence of the protection measures and mechanisms was influenced by the oil tanker-specific demand to comply with the inspection requirements issued by the Oil Companies International Marine Forum (OCIMF) within the Ship Inspection Report Programme (OCIMF, 2019).

5. VULNERABILITY SCANNING OF THE RADARS. Vulnerability scanning is performed to obtain complete insight into the vulnerabilities that are not known only to software vendors, but also to the cyber security community and attackers. The shipboard radar scanning was performed using the world's most widely deployed software tool, Nessus Professional version 8.0.1 (Nessus, 2019). The radars were tested by interconnecting

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

Table 3. Protection measures and mechanisms implemented on the ships.

System	Safeguards	Description	Radar #1	Radar #2
Cyber security management	Security policies and procedures	– Cyber security policy and procedures are part of the Safety Management System – Cyber response plan on board exists – Cyber security policy and procedures are well communicated to the ship's crew – Incident handling procedure is documented – Cyber security policy and procedures are periodically reviewed and audited	√	√
	Crew training and awareness	– Training is conducted by the radar system vendor – Awareness is at a high level	√	√
Radar	Physical protection policy	– Strong access controls are implemented – Access is allowed only to authorised personnel – Hardware interfaces are locked in the radar case	√	√
	Confidentiality agreement	– The agreement is in place	√	√
	Internetworking	– Network connection is not established	√	√
	Authentication policy	– Authentication controls are implemented – Control mechanisms are implemented – Default passwords are changed	√	√
	Cyber security software	– Protection against malware infection and unauthorised use is implemented	√	—

them with a laptop loaded with Nessus Professional vulnerability scanner through an Ethernet cross cable (Figure 3). The remote vulnerability scanning was performed without administrative permissions, while the radar software was running under administrative credentials. Despite the fact that scanning is a passive process that does not influence the radar's functionality, testing was conducted while the ships were docked in port.

5.1. *Radar #1 vulnerability scanning.* The vulnerability scan summary report for Radar #1 including the Internet Protocol (IP) address is shown in Figure 4. In total, three vulnerabilities and 65 pieces of information were detected. The report shows that one vulnerability of critical severity was identified, and two vulnerabilities of medium severity. The most important piece of information found was that the radar software was running on the Microsoft Windows Embedded Standard 7 operating system, updated with Service Pack 1. The embedded operating system installed is a version of the general Windows 7 operating system that allows inclusion of only the components and drivers that are needed for the radar software to function.

The risky vulnerabilities detected are shown in Table 4. The vulnerability identified as critical (Table 4, Vulnerability 1) consists in the fact that vulnerable Server Message

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

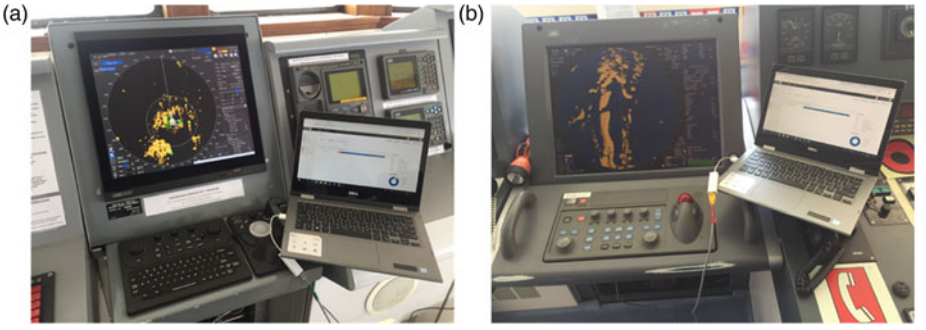

Figure 3. Vulnerability scanning of (a) Radar #1 and (b) Radar #2.

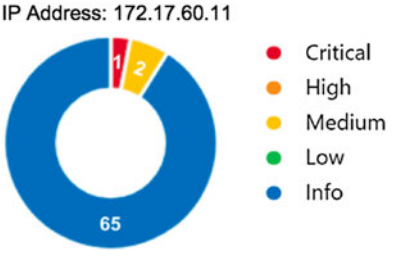

Figure 4. Radar #1 vulnerability scan summary report.

Block service version 1 (SMBv1) was running on the radar. The SMB service provides file and printer sharing, and the vendor's recommended solution is an immediate update with a security patch (Microsoft, 2017). This vulnerability correlates with a well-known maritime industry cyber security incident, the NotPetya global cyber-attack, which targeted the Maersk Line shipping company (CERT CH, 2017). The exploitation of the SMBv1 vulnerability allowed the NotPetya ransomware program to rapidly propagate and execute an arbitrary code on remote target computers (CERT US, 2017). The vendor's recommended solution to update the underlying operating system is quite complex to implement in the shipboard environment. However, a proactive solution would be to secure the radar's underlying operating system setup by blocking the SMBv1, which is actually a redundant service for a device aimed at providing a fixed radar software function in a stand-alone configuration. In the case of Radar #1, the radar manufacturer had integrated an advanced cyber security tool in the radar system, Trend Micro Safe Lock version 1.1 (SafeLock), which allows only application services that have been whitelisted to run. The benefits of blocking unnecessary application services include not only better performance, but also proactive safeguarding from unknown threats and vulnerabilities. However, while the tool proactively enhances the radar's cyber security, it does not provide a solution for vulnerable whitelisted services, as shown by detection of the SMBv1 service (Table 4, Vulnerability 1).

The vulnerabilities identified as medium severity (Table 4, Vulnerabilities 2 and 3) were related to the weaknesses of the services running on the radars' underlying operating system. The vulnerable services allowed remote, unauthorised access and the elevation of privileges. Possible solutions relate to the underlying operating system and involve a secure

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

Table 4. Radar #1 cyber vulnerabilities detected.

	Service	Vulnerability description	Possible solution	Severity
1.	SMBv1 service	Radar #1 is affected by vulnerabilities in the Microsoft Server Message Block version 1.0 (SMBv1) service of the underlying operating system. The most severe of the vulnerabilities could allow a remote attacker to execute code without authentication.	Update the underlying operating system with the vendor's security patch. Secure the underlying operating system setup by blocking the service.	Critical
2.	SMB signing	Radar #1 is vulnerable to man-in-the-middle attacks because signing and security signatures are not required on the SMB service.	Secure the underlying operating system setup by enforcing the signing.	Medium
3.	Remote protocols	Radar #1 is affected by an elevation of privilege vulnerability in remote protocols Security Account Manager and Local Security Authority.	Update the underlying operating system with the vendor's security patch.	Medium

setup and update with a security patch released by the vendor. As in the case of the critical vulnerability detected, the application services locking tool (SafeLock) was shown to be ineffective. It is very important to point out that the implementation of solutions could negatively affect the radar software functionality (IMO, 2004), and should therefore be implemented only by authorised personnel from the radar vendor.

5.2. *Radar #2 vulnerability scanning.* The vulnerability scan summary report for Radar #2 including the IP address shown in Figure 5, indicates that no risky vulnerabilities were detected. The only useful information detected by the vulnerability scan was related to the Ethernet network adapter integrated in the radar. The results were perhaps unexpected as the radar software is running on a system that is about 13 years older than that of Radar #1. In addition, our findings with an ECDIS from the same manufacturer (Svilicic et al., 2019), which is about 3 years older than Radar #1 (the approval dates back to 2013), revealed more significant vulnerabilities compared with Radar #1.

In Radar #2, the radar software was running on Microsoft Windows Compact Embedded .NET version 4.1 operating system that was abandoned when replaced by an updated version (Embedded Standard 7), which is used on Radar #1. This compact version provides a very high level of componentisation by using the operating system components that the radar software requires and leaving out everything else. In addition, hardware the resources of Radar #2 were more modest, with only 48 MB of memory installed (only 2 GB of RAM memory was available on Radar #1). The compact embedded operating system together with the limited hardware resources were the main reasons for Radar #2's very low level of vulnerability to cyber threats.

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

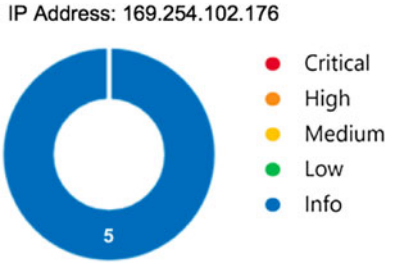

Figure 5. Radar #2 vulnerability scan summary report.

6. RISK LEVEL DETERMINATION. On the basis of the results obtained by means of the on-board survey and vulnerability scan, the identified cyber threats were qualitatively analysed to determine the level of risk. Table 5 shows the identified cyber threats of the radars, together with an estimated impact magnitude level and a likelihood rate. The threat impact level value (from 0 to 100) represents the magnitude of the resulting harm from the vulnerability if successfully exploited. The likelihood rate value (from 0 to 1) represents a probability of the vulnerability exploitation.

In total, eight cyber threats were determined. Five threats were estimated with the highest (total) impact magnitude (Table 5, Threats 1–3, 5, and 8). These threats were related to the maintenance of the radars' underlying operating system (abandoned, out of date and with an insecure setup), and unauthorised access establishment and internetworking. The threats with the highest likelihood rate (a value of 0·6) were associated with the abandoned and outdated operating system of Radar #2. The qualitative risk levels were calculated by multiplying the threat impact magnitude and likelihood. The risk levels were determined on the basis of the multiplication result obtained as follows: (i) acceptable low risk level (multiplication result lower than 25), (ii) medium risk level acceptable over a short period of time (multiplication result between 25 and 50), (iii) high risk level demanding a mitigation plan (multiplication result between 50 and 75), and (iv) critical risk level demanding immediate action (multiplication result higher than 75). The results obtained are given in the cyber risk level radar graph in Figure 6.

The risk level radar graph (Figure 6) shows that two cyber threats are classified as high risk, which demands development of a mitigation plan. The high level threats relate to Radar #2 (Table 5, Threats 1 and 2), and are associated with the underlying operating system, in particular the fact that it has been abandoned and is out of date. The threats imply that an existing vulnerability could be exploited by an attacker with no knowledge about radar systems or expertise in computing technologies (analysed in detail in Section 5). In addition, the first failure of any part of the radar system would most probably lead to migration to a completely new system. In the case of Radar #1, the same threats were classified as medium risk (which was the highest level determined for this radar), which is acceptable over a short period of time. Vendor support for Radar #1's operating system will cease on 13 October 2020, and consequently the risk will rise to critical level if the system is not migrated to the next generation (Microsoft, 2019). The threat from the operating system's insecure setup (Table 5, Threat 3) is associated with a higher risk level for Radar #1 (medium risk level, acceptable for a short time) than Radar #2 (acceptable low risk level). A secure setup of the underlying operating system, which would block unnecessary

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

Table 5. The radars' cyber threats.

	Threat	Description	Radar #1		Radar #2	
			Impact magnitude	Likelihood	Impact magnitude	Likelihood
1	The radar's underlying operating system has been abandoned	Exploitation of the well-known vulnerabilities of the radar's underlying operating system	100	0·4	100	0·6
2	The radar's underlying operating system is out of date	Exploitation of the well-known vulnerabilities of the radar's underlying operating system	100	0·4	100	0·6
3	The radar's underlying operating system insecure setup	Unnecessary services running on the radar reduces performance and opens backdoor for intrusions	100	0·3	100	0·1
4	Crew training and awareness	Crew is unable to perform their duties and responsibilities adequately, and to adhere to operational procedures	50	0·2	50	0·2
5	Unauthorised access	Physical or logical access is allowed for an attacker to target the radar	100	0·1	100	0·1
6	Security policies and procedures	Crew is not familiar with their roles and responsibilities	50	0·2	50	0·2
7	Continuous evaluation and improvement	Lack of ability to respond to rapid technological development	50	0·2	50	0·2
8	Internetworking	Uncontrolled interconnection to external data sources, including both on-ship and off-ship networks	100	0·1	100	0·05

application services, would ensure that radars provide the expected fixed radar software functionality, instead of providing additional file and printer sharing services through the vulnerable SMBv1 protocol, as shown in the case of Radar #1 (Table 4, Vulnerability 1). A reduction in the features of general operating systems would not only provide better radar system performance, but also a proactive solution for safeguarding them from unknown vulnerabilities to ensure long-term functionality. In addition, as in the Radar #1 case, relying on the cyber security tool that allows only application services that have been whitelisted to run could result in serious cyber threats originating from a vulnerable whitelisted service over time.

The low risk level cyber threats determined for both radars (Table 5, Threats 4–7) were associated with unauthorised access controls, crew training and awareness, the development of cyber security-dedicated policies and procedures, and continuous evaluation and improvement. The results were attributed to the radars' operational environments, in particular the fact that the ships were of the same type, sailing on the same routes and managed by the same ship owner. The cyber threat classified as the lowest risk level for each of the

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

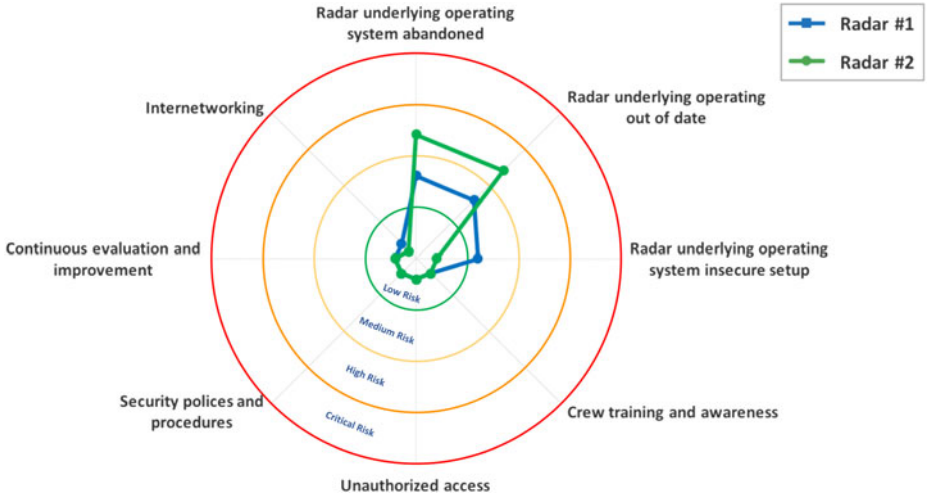

Figure 6. Risk level radar graphs of the radars' cyber threats.

radars related to internetworking to external data sources, including internal ship networks and external off-ship networks (Table 5, Threat 8). The radars were installed in a stand-alone configuration with strong physical protection controls. Therefore, it is very unlikely that internetworking could be established, especially in the case of Radar #2 because of the limited hardware resources. It is worth noting that with the establishment of internetworking, immediate mitigating actions would be needed to ensure the safety and security of shipboard networks according to the requirements of maritime standard IEC 61162-460 (IEC, 2018).

7. CONCLUSIONS. The comparative cyber security resilience estimation of two shipboard radars implemented on SOLAS certified oil/chemical tankers were presented. The radars estimated were chosen from the same manufacturer but were of different generations. The estimation process was adjusted to the radars' operational environment, and conducted by means of ships' crew interviews and a vulnerability scan of the radars' systems. The cyber threats identified were analysed qualitatively, and the analysis revealed eight cyber risks in total. Five threats were classified as an acceptable low risk level, and three as medium and high risk level threats. These were associated with the radars' underlying operating systems, which were abandoned, outdated and had an insecure setup. The acceptable low risk level was attributed not only to the radars' stand-alone configuration (network disconnection), but also to strong unauthorised access controls, crew training and awareness, adherence to security policies and procedures, and continuous evaluation, all of which are traditionally ingrained in tanker shipping.

The results obtained experimentally suggest that potential sources of cyber threats are mainly from the radar software underlying operating system maintenance. The results also suggest that a secure setup of the underlying operating system, which could block unnecessary services, would provide a proactive solution to ensure long-term functionality of the radar software. In addition, the importance of conducting passive vulnerability scanning to identify cyber threats and gain a holistic view of cyber security resilience of shipboard

https://doi.org/10.1017/S0373463319000808 Published online by Cambridge University Press

radars was shown, especially for complex systems with cyber security tools. The results contribute to the understanding of the potential sources of radar system cyber security threats and are applicable to any shipboard software-based system. While maritime regulations are focused on navigation software functionality, the results suggest that there is a need for developing maritime regulations on the cyber security testing of radar software underlying the operating system.

ACKNOWLEDGMENTS

The research was financially supported by the University of Rijeka under the Cyber Security of Maritime ICT-Based Systems research project (Grant No. uniri-tehnic-18-68).

REFERENCES

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

DNV-GL. (2016). *Cyber security resilience management for ships and mobile offshore units in operation*. DNVGL-RP-0496. DNV-GL.

Fernández-Hernández, I., Châtre, E., Chiara, A. D., Da Broi, G., Pozzobon, O., Fidalgo, J., Odriozola, M., Moreno, G., Sturaro, S., Caparra, G., Laurenti, N. and Rijmen, V. (2018). Impact analysis of SBAS authentication. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, **65**, 517–532.

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R. and Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *Journal of Navigation*, **71**, 1025–1039.

International Electrotechnical Commission (IEC). (2018). *Maritime navigation and radio communication equipment and systems - Digital interfaces - Part 460: Multiple talkers and multiple listeners – Ethernet interconnection - Safety and Security*. IEC 61162-460:2018. RLV International Electrotechnical Commission.

International Maritime Organization (IMO). (2004). *Adoption of the Revised Performance Standards for Radar Equipment*. MSC.192(79). International Maritime Organization.

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

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

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

Lewis, S., Maynard, L., Chow, C. E. and Akos, D. (2018). Secure GPS data for critical infrastructure and key resources: cross-layered integrity processing and alerting service. *NAVIGATION, Journal of The Institute of Navigation*, **65**, 389–403.

Microsoft. (2017). *Microsoft Security Bulletin MS17-010 - Critical*. https://technet.microsoft.com/library/security/MS17-010.

Microsoft. (2019). *Microsoft: Search product lifecycle*. 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. (2019). *Tenable Products: Nessus Professional*. https://www.tenable.com/products/nessus/nessus-professional.

Oil Companies International Marine Forum (OCIMF). (2019). *Ship Inspection Report (SIRE) Programme - Vessel Inspection Questionnaires for Oil Tankers, Combination Carriers, Shuttle Tankers, Chemical Tankers and Gas Tankers, Seventh Edition (VIQ 7)*. https://www.ocimf.org/media/127546/SIRE-Vessel-Inspection-Questionnaire-VIQ-Ver-7007.pdf.

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). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Journal of Transportation Security*, **8**, 1–19.

Svilicic, B., Kamahara, J., Rooks, M. and Yano, Y. (2019). Maritime cyber risk management: an experimental ship assessment. *Journal of Navigation*, in press. doi:0.1017/S0373463318001157

Swiss Government Computer Emergency Response Team (CERT CH). (2017). *Notes About The NotPetya Ransomware*. https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware#.

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

United States Computer Emergency Readiness Team. (CERT US). (2017). *Alert (TA17-181A) Petya Ransomware*. https://www.us-cert.gov/ncas/alerts/TA17-181A.