Cyber security risk assessment in autonomous shipping

Tusher, Hasan Mahbub[1]; Munim, Ziaul Haque[1]; Notteboom, Theo E.[2,3,4]; Kim, Tae Eun[5]; Nazir, Salman[1]

[1] Faculty of Technology, Natural and Maritime Sciences, University of South-Eastern Norway.
[2] Maritime Institute, Faculty of Law and Criminology, Ghent University, Belgium.
3 Antwerp Maritime Academy, Belgium.
[4] Faculty of Business and Economics, University of Antwerp, Belgium.
[5] Department of Technology and Safety, University of Tromsø, Norway.

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E. & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, *24*(2), 208-227. https://doi.org/10.1057/s41278-022-00214-0

Cyber Security Risk Assessment for Autonomous Shipping

Hasan Mahbub Tusher[1], *Ziaul Haque Munim*[1*], *Theo E. Notteboom*[2,3,4], *Tae-Eun Kim*[5], *Salman Nazir*[1]

[1] Faculty of Technology, Natural and Maritime Sciences, University of South-Eastern Norway, 3184 Horten, Norway.

[2] Maritime Institute, Faculty of Law and Criminology, Ghent University, 9000 Ghent, Belgium.

[3] Antwerp Maritime Academy, 2030 Antwerp, Belgium.

[4] Faculty of Business and Economics, University of Antwerp, 2000 Antwerp, Belgium.

[5] Department of Technology and Safety, University of Tromsø, 9019 Tromsø, Norway.

*Corresponding author e-mail: ziaul.h.munim@usn.no

Abstract

Autonomous ships would require higher cyber-physical interaction in comparison to traditional shipping operations, thus increasing the vulnerabilities associated with cyber security. The increasing complexity surrounding the innate characteristics of the shipping industry makes it challenging to build a resilient framework for ensuring cyber security. This study proposes a Multi-criteria Decision-Making (MCDM) framework for assessing cyber security risk in the autonomous shipping context. The research was validated through surveying subject matter experts, system designers and seafarers. Different types of equipment and systems are ranked based on their perceived vulnerability to cyber threats. Survey data from 28 subject matter experts are collected and analysed through the Bayesian Best Worst Method (BWM). At system level, the results indicate that navigational systems are the most vulnerable to potential cyber threats, while propulsion systems are the least vulnerable element in the context of future autonomous shipping operations. On a sub-system level, the three most vulnerable parts are Global Navigation Satellite System (GNSS), Electronic Chart Display and Information System (ECDIS), and the communication devices on Shore Control Centres (SCC), while the least vulnerable parts are engine controls, SCC integration platforms and cargo handling at ports.

Keywords: *Maritime operations; Cyber Risk; Unmanned ship; Best-worst method; Risk analysis.*

1. Introduction

Merchant ships have been an integral part of international trade, carrying about 90% of the goods transported globally (*OECD*, 2021). Since its inception, efforts have been made by the stakeholders to make this mode of transport safer, more efficient and more cost effective. The introduction of advanced technologies along with the skills development of the workforce over the years have reportedly increased workplace safety in the maritime domain (Chauvin et al., 2013; *Allianz*, 2020).

Consequently, modern technologies such as Automatic Identification Systems (AIS), Global Navigation Satellite Systems (GNSS), and Electronic Chart Display and Information Systems (ECDIS) have contributed to safer navigation. The increased reliability and efficiency of these technologies has resulted in their broader adoption in the shipping industry such that large ships are now being efficiently operated by fewer crews (Lee & Sanquist, 1996). The notion that it is possible to maintain navigational safety in the future even without any crew onboard has led to the discussion towards the adoption of autonomous shipping technology. Wróbel et al. (2017) stated that the introduction of Maritime Autonomous Surface Ships (MASS) could further reduce the likelihood of navigational accidents, such as collisions and groundings, as human error played a role in the majority of navigational accidents. However, the probability and consequences of non-navigational accidents such as fire and structural failure are likely to increase if no crew members are onboard (Wróbel et al., 2017).

The reduction in operating costs is another contributing factor in the discussion on autonomous shipping since the crew-cost constitutes a substantial part of the vessels' total operating cost (David, 2017). However, no technology is fail-safe and autonomous shipping technology is no exception. Owing to the fact that the most widely used navigational aids such as AIS, GNSS or ECDIS are highly dependent on Global Positioning System (GPS) and VHF-radio communication for their efficient operation, the over-reliance on technology brings its own repercussions and vulnerabilities. Highly automated ships would receive and transmit large amount of data over radio frequency or satellite communication, which make them vulnerable to all kinds of existing threats and risks of the cyber-physical space, in addition to the vulnerabilities of non-navigational accidents onboard (Sen, 2016).

IMO (2017: Annex, p. 1) refers to maritime cyber risk as "*a measure of the extent to which an asset, system, application, or connected infrastructure could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised*".

The cost of cyber-attacks in the industrial sector was estimated to be worth as much as USD 1 trillion with a possibility to double in size every few years, which may vary depending on the calculation methodology used (Sen, 2016). Cyber security is aimed at the protection of hardware, software and associated infrastructure, networks and the data on them, and the services they provide, from unauthorized access, harm, misuse or destruction (Cybok, 2019).

Cyber security in shipping is increasingly becoming multidimensional with threats ranging from activists, competitors, criminals and terrorists (Tam & Jones, 2018). Different cyber threats that pose risk to the maritime industry include illegal extraction, stealing or modification of data to influence the market, damaging or sabotaging ships, smuggling, stealing goods or to kidnap the ship itself (Tam & Jones, 2018). For example, the collision case between US Navy ship USS John S. McCain and an oil tanker was assumed to be the result of possible cyber-attack on the navy ship which altered its navigational signal (Groll, 2017). Shore-based ship management offices are not free from cyber-threats either. One of the top container ship operator A.P. Moller Maersk has experienced a cyber-attack in June 2017 which resulted in hefty losses along with major disruptions in its operations of more than 600 container ships, shore-based offices and several port terminals around the world (Gronholt-Pedersen, 2017). Shipping company BW Group also experienced cyber-attacks in the form of global ransomware in their internal computer system in 2017 (Wei Zhe, 2017).

The increasingly complex global maritime operations and their over-reliance on cyber-space has made it crucial to safeguard against any cyber threats in the system. The management of cyber risks is typically focusing on system or network availability, integrity and confidentiality, also known as the AIC-triad or CIA-triad (Fenrich, 2008; Samonas and Coss, 2014). The notion of availability implies that users can access data, the system or network, when needed or desired. Confidentiality refers to ensuring that information or systems are only accessible to authorized users. Integrity is about preserving information or system accuracy, thereby avoiding unauthorized modification or deletion. Acknowledging the critical nature and possible far-reaching impact of maritime cyber threats, various maritime and port-related organizations and associations have issued guidelines, such as the IMO Guidelines on Cyber Risk Management (IMO, 2017) and the Cyber security Guidelines for Ports and Port Facilities of the International Association of Ports and Harbors (IAPH, 2021).

A recent study by Chang, Kontovas et al. (2021) has found that cyber-attacks are ranked as one of the top hazards in MASS operations. Results from existing research (Kavallieratos, Katsikas et al., 2018) have further identified that AIS, ECDIS, GMDSS as well as human machine interfaces may face higher cyber risks. Autonomous technologies increase the dependency on cyber-physical systems over time and thus increase the need for protection against potential cyber threats. Therefore, maritime stakeholders are challenged to take appropriate precautions against cyber threats, among many other repercussions that emerge from a possible wider adoption of autonomous technologies.

As such, effective cyber risk management constitutes a competitive and operational strategy, imperative for the implementation and operation of MASS. The identification of possible maritime cyber threats and risks is the first step towards their minimization and a key aspect of effective cyber risk management. Consequently, existing and emerging cyber threats should be identified and be weighed against their potential negative effects on corresponding branches within the industry.

This study aims to identify the most, as well as the least, vulnerable areas of cyber threats related to autonomous technologies, both on ships and shore-based facilities. In addition, recommendations are presented to provide guidance on the areas in the maritime industry which need to be prioritized in terms of implementation of safeguards against cyber threats.

The study is structured as follows. The next section provides a literature review on possible sources of cyber threats in the maritime field with regard to MASS. Next, we use the identified risks as input in a Multi-criteria Decision-Making (MCDM) framework for assessing cyber security risk in the autonomous shipping context. Using a survey setup, different types of equipment and systems are ranked based on their perceived vulnerability to cyber threats. The results of this empirical exercise are presented in section 4. We conclude the paper with a discussion of the findings and the formulation of recommendations on cyber security within the context of MASS.

2. Literature review

2.1. Autonomous ships and cyber security

The International Maritime Organization (IMO) as well as different classification societies (Lloyd's Register, DNV etc.) have categorized autonomous ships based on their operational characteristics and level of human involvement. These categories stem from a conceptual framework ranging from "manual" ships with seafarers onboard to "fully-autonomous" ships without any human presence onboard (*DNV* 2018; Maritime *UK*, 2018; Lloyd's Register, 2017). Since connectivity between ship and shore infrastructures is the main enabler of autonomous and remote-controlled technologies, cyber security would play a crucial role in ensuring the operational efficiency of these ships. This study focuses on the defined concept of degree-3 autonomous ships by IMO where the ships will be remotely controlled from a shore control centre (SCC) without any seafarer onboard.

2.2. Types of cyber threats

The motivation for the criminals carrying out cyber-attacks may involve gaining unauthorized access to crucial assets; theft or smuggling of cargo and other activities related to terrorism, piracy, espionage, ransom or war (Sen, 2016). While most maritime threats have a physical form like piracy or theft, cyber security threats are latent in nature resulting in disruption in operation and loss or damage of goods and the environment (Jones et al., 2016). A literature review has therefore been performed to identify the most common cyber security threats that have been discussed with regards to the future autonomous ship.

To identify the criteria and sub-criteria for the analysis of cyber security risk in the autonomous shipping domain, a systematic literature search was conducted in the Scopus database. The initial keyword search involved the Boolean expression — ("autonomous ship*" OR "autonomous vessel*" OR "maritime autonomous surface ship*") AND ("cyber security" OR "cyber risk"). The literature search resulted in 20 relevant studies. A keyword frequency analysis of these studies suggested three additional keywords: unmanned ship, cyber physical system and security systems. Therefore, a revised search was conducted using the following search criteria: ("autonomous ship*" OR "unmanned ship*"OR "autonomous vessel*" OR "maritime autonomous surface ship*") AND ("cyber security" OR "cyber-security" Or "cybersecurity" OR "cyber risk" OR "cyber physical system" OR "security system*"). This second round returned 35 records for consideration. After manually screening for relevance, 17 studies were retained. In addition, 08 relevant studies were identified through snowballing of cited references of these 17 studies.

A plethora of cyber security threats that exist today in the maritime landscape emerged from the literature review. The integration of digital technologies within the communication paradigm brings about obvious risks as we move from a traditional mode of operation to more advanced remote or autonomous ship operation. The potential emergence of autonomous and crewless vessels and their efficient operation in the future would fully rely on the inter-connected network between ship and SCC or with other ships in the vicinity, thereby increasing the risk of cyber-attacks (Kavallieratos, Diamantopoulou, et al., 2020; Tam & Jones, 2018). The operational characteristics and the transportation model of MASS would include remote controlled operation centres, onboard vessel management (e.g., robotic propulsion system, obstacle and collision avoidance systems etc.) along with other shore-based support systems (Heffner & Rødseth, 2019). However, not all segments within the maritime industry are equally susceptible to the same type of cyber threats. For example, fake Global Positioning System (GPS) signals or breaches in ships' ECDIS have entirely different outcomes than a cyber security breach in the cargo management system onshore or in the port infrastructure.

It is evident that both the shipboard and the shore-based operations are susceptible to cyber risks. Therefore, it is crucial to understand which areas of operations are most vulnerable. The different types of cyber security threats analysed from the literature in the maritime domain can be classified into five major categories for the ease of weighing the vulnerability against each other in the later part of the study. These categorizations of vulnerable areas include navigational systems, propulsion control systems, port operations, shore control centre and shore-based management offices as described below.

2.2.1. Threats to Navigational Systems

The sole reliance on satellite systems for efficient vessel navigation makes them the most exposed target for any type of cyber threat. Global Navigation Satellite System (GNSS), Global Positioning Systems (GPS), Automatic Identification Systems (AIS) and Electronic Chart Display and Information System (ECDIS) are some of the widely used navigational equipment onboard, all of which operate on the principle of signal processing and transmission, thereby bearing the risk of being subjected to cyber-attacks (Dyryavyy, 2015). Moreover, the interdependence of navigational equipment with each other for their normal operation makes it crucial to keep all systems safe against any type of threat (Svilicic et al., 2019). Jamming and spoofing are some of the most common types of cyber threat to navigational systems. Electronic signals to and from the navigational equipment can be *jammed*, where information could be intercepted and used maliciously. Competing signals can be transmitted deliberately to prevent accurate reception of data from satellites, thus jamming communication devices. *Spoofing* introduces false signals thereby compromising the reliability of navigational equipment used (Androjna et al., 2020). These types of signal interference have the potential to shift the course of navigation, obfuscation, theft, damage or denial of service which have far greater consequences on autonomous ships than in conventional ones (Androjna et al., 2020; Jones et al., 2016).

2.2.2. Threats in Propulsion Control Systems

Ship propulsion control systems are vulnerable to cyber threats due to their dependence on information and communication technologies. Kavallieratos et al (2019) envisaged a system architecture for autonomous shipping where ship propulsion or Engine Automation System (EAS) is comprised of three sub-layers: Autonomous Engine Monitoring and Control systems – AEMC, the Engine Efficiency System – EES, and the Maintenance Interaction System – MIS, all of which take advantage of information and communication technologies to function. Other emerging autonomous shipping technologies also involve the inclusion of computer-based communication technologies in propulsion systems (Jones et al., 2016). Therefore, it is evident that these technologies are liable to similar consequences with regard to cyber threats. The use of outdated software, lack of adequate safeguards against cyber threats, and lack of training and expertise could potentially increase the cyber security risks associated with propulsion systems (Chang et al., 2019; Gallagher, 2015).

2.2.3. Threats in port operations

Cargo vessel operations in ports and the broader organisation of the maritime-land interface in supply chains largely depends on safe and secure port operations. Drug smuggling, theft of high profile cargo, remote access to the terminal management system, bypassing customs, breaching the cargo tracking program, are some of the common threats in ports which have a high association with cyber-criminal activities (*CyberKeel*, 2014). Cyber threat perpetrators might try to exploit skill shortages necessary for supporting and securing complex systems in ports, weaknesses in the security architecture, and software vulnerabilities (IAPH, 2021). Commonly used and data-rich integrated electronic platforms, such as Port Community Systems (PCS) and systems related to Maritime Single Windows (MSW), might be particularly targeted by cyber criminals.

Mooring of inbound and outbound ships in ports is one of the crucial operations, and a prerequisite for the safe docking of the ship and the start of cargohandling operations. Modern mooring technology can be remotely controlled via radio signals which are vulnerable to cyber threats (Schmidt et al., 2016; Tam & Jones, 2018). In addition to the security breaches in radio communication and software, new types of hardware hacking in barcode scanners and other types of devices are used to instigate cyber-criminal activities in port operations (Balduzzi et al., 2013; Jones et al., 2016; *CyberKeel*, 2014).

2.2.4. Threats in Shore Control Centre

Shore Control Centres (SCC) would be the core part in the operations of autonomous ships. Crewless shipping would only be possible if the ship-to-shore communication; reliance on sensor data; and safe and secure signal processing across different devices, is ensured with proper safety and redundancy. However, there is no consensus on the desired system architecture of future autonomous ships (Kavallieratos et al., 2019). As a result, determining the cyber threats on shore control centres is a challenge. Several potential areas of a breach have been identified in literature, within the remote manoeuvring support system. For example, there are high risks associated with changes in user credentials, or administrative access and loss of connection availability, medium risks with data tempering, and comparatively lower risks with confidentiality breaches in the SCC (Kavallieratos et al., 2019). Tam & Jones (2018) presented a risk assessment framework to understand the maritime cyber risk in future autonomous ships, employing sensor networks and remote access. Future studies are expected to pinpoint emerging cyber threats related to SCCs. More studies are needed since modelling data is scarce at the moment, and in-depth analysis is restricted to initial assessment only.

2.2.5. Threats in Shore-based Management Offices

The rise in online cargo bookings and real-time communication with ships, suppliers and ship agents have increased reliance on the internet and thus potentially increased the associated risks. The largest shipping companies of the world, such as CMA-CGM, MSC, Maersk and Carnival cruises, and even the IMO offices, have been victims of cyber-attacks (Lars, 2021). Deleting cargo information related to rates, loading, stowage plan etc., are some of the major concerns for any shipping company, striving to keep their maritime supply chain intact and safe. The financial, as well as reputational, losses are significant owing to such situations. The “icefog” attack on Japanese and Korean shipbuilders to extract restricted documents in 2013, and the notorious “NotPetya” cyber infection at Maersk’s headquarters in June 2017, are some of the examples how shore-based offices can fall victim to cyber-attacks (Gronholt-Pedersen, 2017; *CyberKeel*, 2014).

The generation of fake invoices, forced encryption, social media hacking, fake websites, ransomware, Trojan attacks, data manipulation, information theft and industrial espionage are some of the most common types of cyber threats that shore-based management offices are vulnerable to (Androjna et al., 2020; Chang et al., 2019; *CyberKeel*, 2014).

The identified cyber security risks from the literature are consolidated in Table 1.

Table 1: Cyber security threats in different segments of future autonomous ships

SL	Criteria	Sub-criteria	References
1.	Navigational system (NGS)	Global Navigation Satellite System (GNSS)	(Androjna et al., 2020; Balduzzi et al., 2013; Bolbot et al., 2020; Bothur et al., 2017; Dyryavyy, 2015; Gallagher, 2015; Jones et al., 2016; Kardakova et al., 2020; Kavallieratos, Diamantopoulou, et al., 2020; Svilicic et al., 2019)
		Electronic Chart Display and Information System (ECDIS)	
		Radio Detection and Ranging (RADAR)	
		Automatic Identification System (AIS)	
2.	Propulsion control system (PCS)	Engine control (ENG)	(Bolbot et al., 2020; Kavallieratos, Diamantopoulou, et al., 2020)
		Sub-system control (SSC)	
		Control room integration (CRI)	
		Logging and data management (LDM)	
3.	Port-operations (PO)	Berthing (BER)	(Androjna et al., 2020; Chang et al., 2019; Jones et al., 2016; Senarak, 2020)
		Cargo handling (CH)	
		Documentation (DOC)	
		Clearance and forwarding (CF)	
4.	Shore Control Centre (SCC)	Sensors and control equipment (SCE)	(Bolbot et al., 2020; Kavallieratos, Diamantopoulou, et al., 2020)
		Data management system (DMS)	
		Integration platform (IP)	
		Communication devices (CD)	
5.	Shore-based management offices (SMO)	Expired software (ES)	(Androjna et al., 2020; Chang et al., 2019; Gallagher, 2015; Svilicic et al., 2019)
		Phishing emails (PM)	
		USB sticks (USB)	
		Local servers (LS)	

3. Methodology

3.1. MCDM Method

We employ the Bayesian variant of the Best-Worst Method (BWM) in the cyber security risk assessment of autonomous ships. BWM is a variant of the MCDM method, which has several advantages over other MCDM methods, particularly w.r.t. reduced requirements for pair-wise comparisons and improved consistency. MCDM methods are widely used in risk assessment in different contexts, such as environmental risk (Jozi et al., 2015), project risk (Ali et al., 2019; Wang & Elhag, 2006), ergonomic risk (Delice & Can, 2020), financial risk (Kou et al., 2014), marine machinery risk (Emovon et al., 2015) and ship collision risk (Silveira et al., 2021). Commonly used MCDM methods include AHP, ANP, TOPSIS, VIKOR, SAW, DEMATEL, PROMETHEE, ELECTRE, and their variants (Zavadskas et al., 2014). Rezaei

(2015) first proposed the BWM, and Mohammadi & Rezaei (2020) later introduced the Bayesian BWM which allows probabilistic group decision-making.

3.2. Data collection

Based on the identified criteria and sub-criteria for cyber security risk for autonomous ships (see Table 1), we designed and distributed a web-survey using nettskjema.no. To ensure anonymity of respondents, the survey did not collect any personal data. The survey was distributed through the professional networking site ‘LinkedIn’. Collecting data using LinkedIn is a practice that was also used in other studies, see for example Kaliszewski et al. (2021). The survey was distributed through the authors’ LinkedIn networks and in several groups of maritime professionals. Between March and May 2021, 37 responses from maritime professionals were recorded. After screening the observations, four survey responses were removed due to incompleteness, three due to straight lining, and two due to inconsistent response patterns. Hence, 28 observations were used in the analysis. Table 2 presents an overview of the respondents’ profiles.

Table 2: *Overview of respondents*

Country (Job)	**Frequency**	**Position (Job)**	**Frequency**
Argentina	1	Classification society representative	1
Bangladesh	4	Management level seafarer (Engineering)	2
Belgium	1	Management level seafarer (Navigation)	5
Germany	1	Marine instructor/ teacher	3
Holland	1	Operational level seafarer (Engineering)	8
India	1	Operational level seafarer (Navigation)	6
Iran	1	Maritime Researcher	3
Japan	1	**Total**	**28**
Malaysia	1		
Malta	1	**Years of experience**	
Norway	9	Average	10.43
Poland	1	Minimum	2.00
Singapore	3	Maximum	24.00
Sweden	1	Standard deviation	5.80
United Kingdom	1		
Total	**28**		

3.3. Bayesian BWM

The Bayesian BWM can be implemented in the following five steps:

Step 1. Identification of cyber security risk criteria and their sub-criteria

In Section 2, five criteria for cyber security risk assessment were identified as (1) Navigational system, (2) Propulsion control system, (3) Port operations, (4) Shore Control Centre, and (5) Shore-based management offices. Under each criterion, four underlying sub-criteria were identified. Figure 1 presents the MCDM framework for cyber security risk assessment for autonomous shipping.

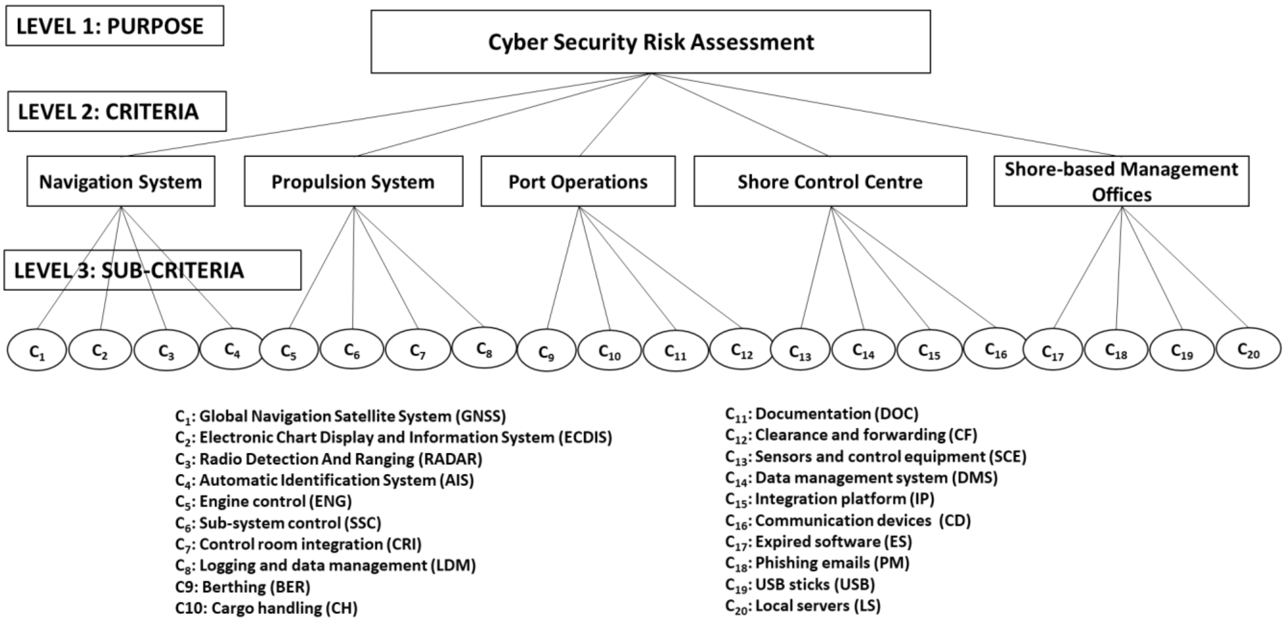

LEVEL 1: PURPOSE
Cyber Security Risk Assessment
LEVEL 2: CRITERIA
Navigation System
Propulsion System
Port Operations
Shore Control Centre
Shore-based Management Offices
LEVEL 3: SUB-CRITERIA
C_1
C_2
C_3
C_4
C_5
C_6
C_7
C_8
C_9
C_{10}
C_{11}
C_{12}
C_{13}
C_{14}
C_{15}
C_{16}
C_{17}
C_{18}
C_{19}
C_{20}
C_1: Global Navigation Satellite System (GNSS)
C_2: Electronic Chart Display and Information System (ECDIS)
C_3: Radio Detection And Ranging (RADAR)
C_4: Automatic Identification System (AIS)
C_5: Engine control (ENG)
C_6: Sub-system control (SSC)
C_7: Control room integration (CRI)
C_8: Logging and data management (LDM)
C9: Berthing (BER)
C10: Cargo handling (CH)
C_{11}: Documentation (DOC)
C_{12}: Clearance and forwarding (CF)
C_{13}: Sensors and control equipment (SCE)
C_{14}: Data management system (DMS)
C_{15}: Integration platform (IP)
C_{16}: Communication devices (CD)
C_{17}: Expired software (ES)
C_{18}: Phishing emails (PM)
C_{19}: USB sticks (USB)
C_{20}: Local servers (LS)

Figure 1: *Cyber security risk assessment framework for autonomous shipping*

Step 2. Identification of the most vulnerable (MV) and the least vulnerable (LV) criterion and sub-criterion

In the BWM survey, respondents identified the most vulnerable (MV) and the least vulnerable (LV) criterion. Table 3 reports the MV (column two) and LV (column eight) for the five criteria. The MV and LV for their respective sub-criteria were also identified, see supplementary datafile in Excel format.

Step 3. Comparison of the most vulnerable (MV) against other criteria (j)

After selecting the most vulnerable (MV) criterion, the respondents were asked to compare the (MV) with other criteria on a 1 to 9 scale, in which 1 refers to equally vulnerable compared to the other criterion, and 9 refers to absolutely more vulnerable than the other criterion. This forms the most vulnerable-to-others (MVO) vector:

$X_{MV} = (x_{MV1}, x_{MV2}, \ldots, x_{MVn})$; here, x_{MVj} illustrates the preference of the most vulnerable criterion MV over criterion j, and x_{MVMV}=1.

Step 4. Comparison of other criteria (j) with the least vulnerable criterion (LV)

After selecting the least vulnerable (LV) criterion, respondents were asked to compare the other criteria with it on a 1 to 9 scale, in which 1 refers to equally vulnerable compared to the (LV) criterion and 9 refers to absolutely more vulnerable than the (LV) criterion. This forms the others-to- least vulnerable (OLV) vector:

$X_{LV} = (x_{1LV}, x_{2LV}, \ldots, x_{nLV})$; here, x_{jLV} illustrates the preference of other criterion j over the least vulnerable criterion LV, and x_{LVLV}=1.

Table 3: *Criteria level MVO and OLV vectors*

No	MV	NGS	PCS	PO	SCC	SMO	LV	NGS	PCS	PO	SCC	SMO
1	NGS	1	4	7	5	5	PO	7	5	1	4	4
2	NGS	1	1	1	1	3	SMO	9	7	5	7	1
3	NGS	1	9	9	7	3	PCS	9	1	3	3	5
4	SMO	5	4	3	3	1	NGS	1	3	4	5	5
5	NGS	1	3	5	4	7	PO	5	4	1	3	1
6	NGS	1	7	3	4	5	PO	9	7	1	5	6
7	SMO	9	9	3	1	1	NGS	1	1	3	9	9
8	NGS	1	7	7	7	5	SMO	5	5	5	7	1
9	NGS	1	7	9	1	1	PCS	9	1	7	9	7
10	SMO	5	3	7	7	1	PCS	3	1	3	3	3
11	NGS	1	3	5	9	7	PCS	7	1	9	9	7
12	NGS	1	4	7	7	7	PO	7	7	1	4	4
13	PCS	5	1	3	3	3	SMO	5	5	1	3	1
14	NGS	1	5	3	5	3	PCS	5	1	1	1	1
15	NGS	1	5	3	3	3	PCS	2	1	2	2	2
16	NGS	1	3	3	5	5	SMO	5	5	3	3	1
17	NGS	1	3	3	5	3	SCC	4	3	4	1	4
18	NGS	1	3	5	7	7	SMO	7	5	5	5	1
19	SMO	5	2	4	4	1	PCS	3	1	3	3	2
20	SCC	7	7	4	1	2	PCS	3	1	7	8	7
21	SCC	5	5	1	1	1	NGS	1	3	5	9	9
22	SMO	3	3	3	1	1	PCS	7	1	3	3	3

23	NGS	1	5	5	3	3	PCS	5	1	3	5	5
24	NGS	1	3	3	7	7	PCS	9	1	9	9	9
25	SCC	5	7	6	1	4	PO	7	7	1	8	8
26	NGS	1	7	5	2	1	PCS	9	1	7	6	7
27	NGS	1	9	7	7	7	SCC	9	7	9	1	1
28	NGS	1	3	5	2	4	PO	9	7	1	8	6

MV: Most vulnerable, LV: Least vulnerable; NGS: Navigational system, PCS: Propulsion control system, PO: Port-operations, SCC: Shore Control Centre, SMO: Shore-based management offices.

Step 5. Estimate w^r , that is the weight for each respondent, $r = 1, \dots, 29$. Then, applying the Bayesian BWM, the aggregate weights of all respondents $w^* = w_1^*, w_1^*, \dots, w_n^*$ are estimated.

$$\begin{aligned} A_{MV}^r \mid w^r \sim M\left(\frac{1}{w^r}\right), \forall r = 1, \dots, r \\ A_{LV}^r \mid w^r \sim M(w^r), \forall r = 1, \dots, r \\ w^r \mid w^* \sim D(\gamma \times w^*), \forall r = 1, \dots, r \\ \gamma \sim G(0.1,0.1) \\ w^* \sim D(1) \end{aligned} \qquad (1)$$

Here, M and D represent a multinomial and a Dirichlet distribution, respectively. G (0.1,0.1) stands for a gamma distribution with the shape parameters of 0.1. Estimation of equations set (1) requires a Markov-chain Monte Carlo (MCMC) sampling (Gilks, Richardson, & Spiegelhalter, 1995). We employ the Bayesian BWM using *JAGS: Just Another Gibbs Sampler* (Plummer, 2004)[1]. The solution is a creedal ranking representing a probabilistic comparison of a set of criteria visualized through directed graphs (Mohammadi & Rezaei, 2020) (see Figure 2). Figure 3 reports the global weights on the sub-criteria level calculated by multiplying the aggregate criteria level weights with their respective sub-criteria level weights.

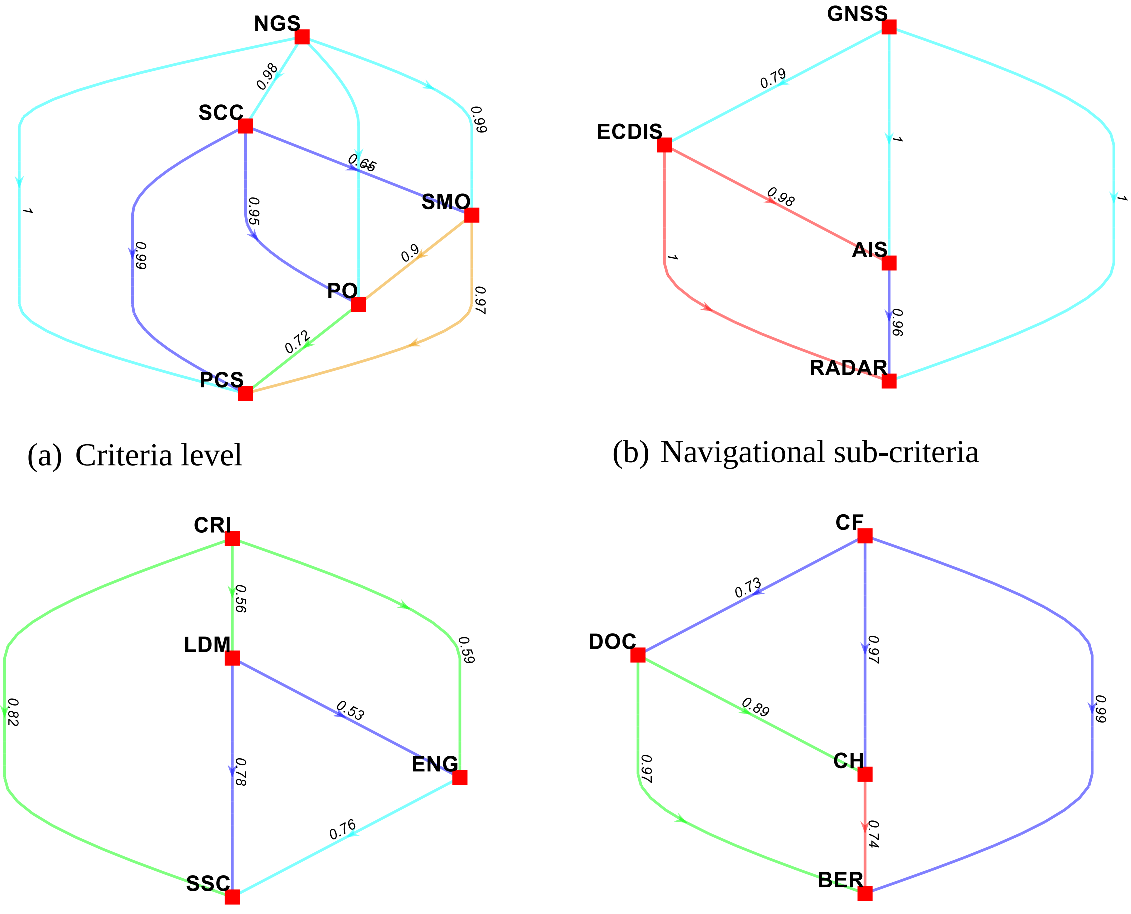
4. Results

The cyber security risk of the criteria and sub-criteria for autonomous shipping are estimated using the Bayesian BWM and reported in Figure 2. Figure 2(a) reveals that navigational system is the most vulnerable one, followed by shore control centre, shore-based management offices,

[1] Open source version available at https://github.com/Majeed7/BayesianBWM

port operations and propulsion control system. The values on the edges of the directed graph can be interpreted as the confidence level of the rankings (Mohammadi & Rezaei, 2020). For instance, one can say with 100% confidence that the navigational system is considered more vulnerable to cyber-attack than propulsion control system, while with 72% confidence it can be said that port operations is more vulnerable than propulsion control system.

Among the sub-criteria for navigational system, GNSS is considered by respondents as the most vulnerable to cyber-attack, while RADAR is the least vulnerable [see Figure 2(b)]. Under propulsion control system, "control room integration" is the most vulnerable and "sub-system control" is the least vulnerable [see Figure 2(c)]. For port operations, "clearance and forwarding" operation is the most vulnerable and "berthing" is the least [see Figure 2(d)]. For shore control centre, "communication devices" are the most vulnerable and "integration platforms" are the least [see Figure 2(e)]. Finally, at shore-based management offices, "phishing emails" are identified as the most vulnerable and "expired software" the least vulnerable [see Figure 2(f)].

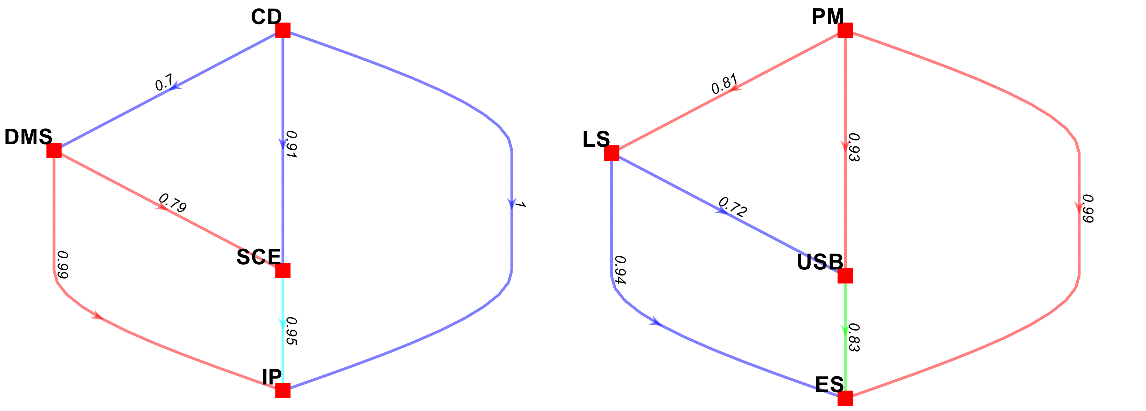


(a) Criteria level

(b) Navigational sub-criteria

(c) Propulsion control sub-criteria

(d) Port operations sub-criteria



(e) SCC sub-criteria

(f) Shore-based mgt. offices sub-criteria

Figure 2: *Credal ranking of criteria (a) and their sub-criteria (b-f).* ***(CRITERIA)*** *NGS: Navigational system, PCS: Propulsion control system, PO: Port-operations, SCC: Shore Control Centre, SMO: Shore-based management offices.* ***(SUB-CRITERIA)*** *GNSS: Global Navigation Satellite System, ECDIS: Electronic Chart Display and Information System, RADAR: Radio Detection and Ranging, AIS: Automatic Identification System; ENG: Engine control, SSC: Sub-system control, CRI: Control room integration, LDM: Logging and data management; BER: Berthing, CH: Cargo handling, DOC: Documentation, CF: Clearance and forwarding; SCE: Sensors and control equipment, DMS: Data management system, IP: Integration platform, CD: Communication devices; ES: Expired software, PM: Phishing emails, USB: USB sticks, LS: Local servers.*

Global weights on the sub-criteria level provide insights into the overall ranking of the most vulnerable parts in the autonomous shipping system, as reported in Figure 3. Five of the most vulnerable parts are GNSS, ECDIS, CD, AIS and PM. Here, three of these, i.e., GNSS, ECDIS and AIS, belong to the navigational system criterion. CD belongs to the shore control centre and PM to the shore-based management office. The five least vulnerable parts are ENG, IP, CH, SSC and BER. Two of these, i.e., ENG and SSC, come under propulsion control system; another two, CH and BER are sub-criteria in port operations; and only IP is from the criterion *shore control centre*.

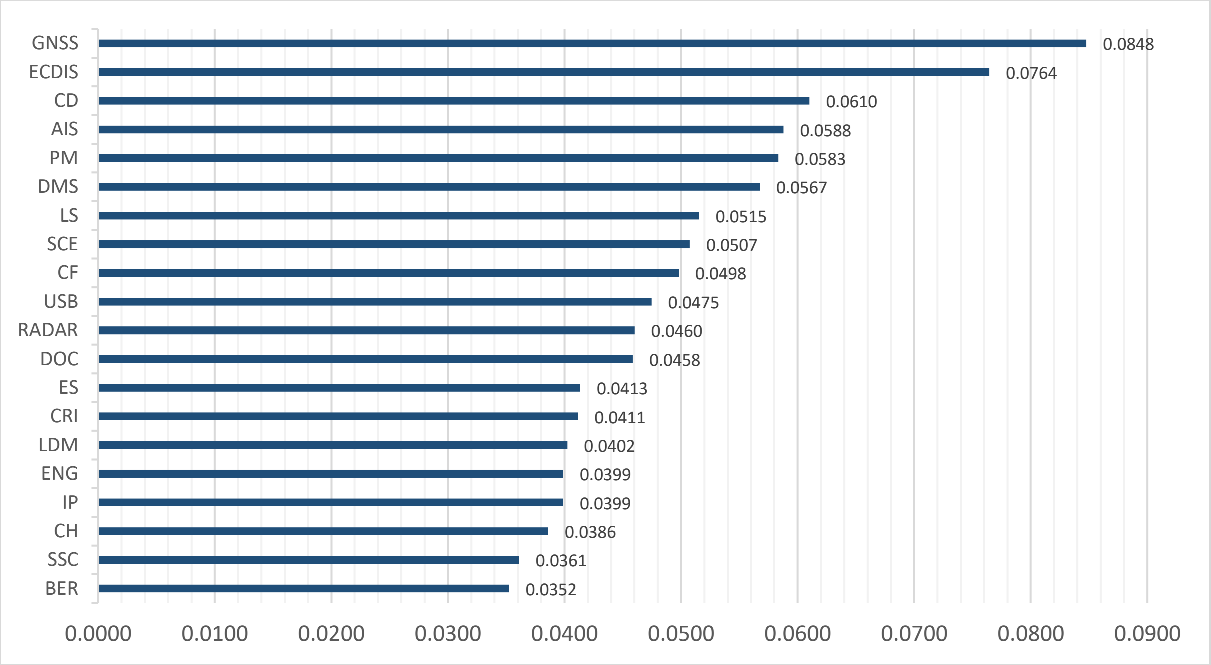


Figure 3: *Global weights of sub-criteria.* ***(CRITERIA)*** *NGS: Navigational system, PCS: Propulsion control system, PO: Port-operations, SCC: Shore Control Centre, SOM: Shore-based management offices.* ***(SUB-CRITERIA)*** *GNSS: Global Navigation Satellite System, ECDIS: Electronic Chart Display and Information System, RADAR: Radio Detection and Ranging, AIS: Automatic Identification System; ENG: Engine control, SSC: Sub-system control, CRI: Control room integration, LDM: Logging and data management; BER: Berthing, CH: Cargo handling, DOC: Documentation, CF: Clearance and forwarding; SCE: Sensors and control equipment, DMS: Data management system, IP: Integration platform, CD: Communication devices; ES: Expired software, PM: Phishing emails, USB: USB sticks, LS: Local servers.*

5. Discussion

5.1. Evaluation of the findings

The Bayesian BWM analysis operationalized in this study identifies the most- and the least-vulnerable systems that could be potentially exposed to cyber-security threats in autonomous shipping operations. Since the development of autonomous shipping technologies and associated discussions are still in their infancy, this study delineates a holistic view of the cyber-security threats. It is evident that the potential proliferation of interconnected cyber-physical systems would increase security challenges (Kavallieratos, Katsikas, et al., 2020). The notion can be further justified by observing the global weights of the sub-criteria in Figure 2, where satellite communication systems and associated equipment, relying on integrated communication infrastructure, have the highest potential to be affected by contemporary cyber-threats. Moreover, the elements related to communication at the sub-criteria level are also in the higher risk zone (e.g., communication devices in shore control centre and phishing emails in shore-based management offices). On the other hand, operations that are independent in nature, i.e., they do not rely heavily on integrated communication solutions, such as berthing and sub-system controls, bear the least risk.

It is also evident that the navigational system as a whole is more susceptible to cyber-threats than any other criteria. Our findings are in line with those of other studies which also point to the heightened vulnerability of the ship navigational systems (Ahvenjärvi et al., 2019; Alop, 2019; Bolbot et al., 2020). The presented methodological framework, as well as the estimated global weights, can be used directly in decision-making by shipowners while choosing autonomous ship alternatives. Furthermore, our results provide some guidance to shipping companies, in terms of taking preventive measures to reduce the risk of the more vulnerable segments in ship operations.

5.2. Implications for the maritime industry

Autonomous ships are a novel addition to the present maritime landscape. Existing navigational aids, such as GPS and gyrocompasses, are used during autopilot operations that also include raw data from GNSS and subsequent processing in the inertial motion units (IMU) and Kalman filtering for accurate positioning of ships (Felski & Zwolak, 2020). Reliance on such equipment will increase manyfold in the context of autonomous shipping operations.

Cyber threats have been identified as one of the major vulnerabilities of GNSS in previous literature (GPS World, 2016). Our study confirms this finding.. To minimize and overcome such threats, earlier studies have proposed standard threat reporting and integrated threat monitoring systems, where information about detected jamming events for GNSS are shared in a centralized server which is accessible to users in view of taking real-time actions (Thombre et al., 2018).

Moreover, nowadays, built-in jamming threat signalling mechanisms for GPS receivers, or receivers with multi-segment, controlled antenna, that eliminate jamming signals are also available (Felski & Zwolak, 2020). The maritime industry could take advantage of such systems and integrate niche vulnerabilities, reported by maritime users (e.g., ships, ports, maritime research centres etc.) to minimize the threat perception in GNSS and autonomous navigation. In addition, outputs from research projects like STRIKE3 and DETECTOR, funded by the European Commission (Thombre et al., 2018), could be employed to minimize jamming and spoofing interferences in GNSS infrastructure. More of such research could potentially lead to a robust and risk-free environment for GNSS usage in maritime autonomous ships.

In this context, ship-to-ship as well as ship-to-shore communications would subsequently follow new technology and newer frameworks, which must pass through sufficient testing and validation. However, considering the emerging cyber-security risks due to extensive reliance on public networks (4G, 5G, satellite etc.), and high exposure to external systems (e.g., in shore control centres and other shore-based infrastructures) (Bolbot et al., 2020), we argue that current maritime practices should be adjusted to suit the evolving scenario of autonomous shipping in order to maintain the sustainable future of the maritime industry. Going forward, increased implementation of Internet-of-Things (IoT), based on blockchain technology platforms for managing MASS operations, might mitigate vulnerability to cyber security to some extent (Munim et al., 2021).

In addition, existing maritime threats at sea could evolve in the form of hacktivism, cyber criminality, cyber espionage, cyber terrorism and cyber war. These could compromise vessel navigation, propulsion and supply chain, resulting in costly downtime and financial losses (Androjna et al., 2020; Jones et al., 2016; Senarak, 2020). Social media hacking, fake website, phishing emails and similar forms of cyber-threats could also increase the vulnerabilities to shore-based as well as shipboard systems (Androjna et al., 2020; Chang et al., 2019). A combination of these issues is termed "hybrid threats", requiring societal awareness, resilience and good personal cyber security practices to best defend against them (Androjna et al., 2020; European Union, 2020; American Club, 2020). The American P&I Club, along with other stakeholders recommends that ship management companies, as well as regulatory authorities, should identify roles and responsibilities of personnel and systems, and implement technical and procedural measures, along with appropriate contingency plans to counteract potential cyber threats (American Club, 2020).

The purpose of autonomous shipping is to reduce costs and increase reliability (Zaccone, 2021). This would not be sustainable if reliability were to be compromised by cyber-threats. Financial losses, damage of goods and legal issues arising from cyber-threats would ultimately hamper the adoption of autonomous systems in the maritime industry. Therefore, a cyber-secure environment is not only essential, but also critical to ensure flawless future maritime operations. In an attempt to safeguard the emerging as well as future cyber-security threats, classification societies and international regulators are putting objective measures in place. DNV provides best practices (DNV-GL, 2016) on how to avoid cyber mishaps onboard, and ashore. In addition, recent amendments in the International Safety Management code (ISM) by the IMO (DNV, 2019) manifest the willingness to ensure a safe and efficient shipping and also support the adoption of safe and efficient autonomous shipping.

6. Conclusions

This study has presented an integrated approach to elicit cyber-security vulnerabilities in the context of future autonomous shipping. Our results suggest that navigational systems are the most vulnerable to cyber-threats, whereas propulsion control systems are the least. This necessitates communication devices and protocols used for the navigation of autonomous ships be redundant and cyber-safe. Other emerging new systems in the context of autonomous ships, such as the shore control centre and associated equipment, although opaque for the time being, are potentially vulnerable to multidimensional cyber-threats as described in this study. The unpredictable nature of cyber-security threats, along with inherent repercussions, call for a multifaceted approach to safeguard the future of shipping. A pre-emptive approach should include not only technical guidelines, but also policy and industrial ones, and best practices in risk management, and in the behavioural and cultural aspects of shipping. In addition, experts concur that only compliance-based actions would not be sufficient to safeguard against cyber threats. Rather, an all-out comprehensive approach, considering the above aspects, would ensure a safe and secure adoption of autonomous shipping.

This study was an attempt to elicit an overview of the potential cyber-vulnerabilities ranked in the context of future autonomous maritime operations by applying a Multi-criteria Decision-Making (MCDM) framework.

Future studies aimed at precautions and compliance related to cyber-readiness would gain traction with regard to autonomous shipping. The cyber security risk assessment framework proposed here can be extended by incorporating emerging criteria and sub-criteria. Future study should also explore the corresponding cyber security control and management strategies to mitigate and/or reduce the impact of the identified threats. In addition, focused studies involving the human factor, behavioural aspects and training related to software engineering and cyber-attack defence skills would be necessary as we advance towards a more integrated environment involving human and machine in complex systems of autonomous shipping operations.

Acknowledgement

The authors thank the Editor-in-Chief Professor Hercules Haralambides and the handling editor for their valuable feedback on earlier versions of the study. The authors' contribution in this study are as follows: Tusher H. M: Conceptualization, Survey design, Data collection, Writing – original draft, Writing – revised draft. Munim Z. H: Conceptualization, Data collection, Methodology, Formal analysis, Writing – original draft, Writing – revised draft. Notteboom T. E: Validation, Writing – original draft, Writing – revised draft. Kim T-E: Data collection, Writing – revised draft. Nazir S: Validation, Writing – revised draft.

References

Ahvenjärvi, S., I. Czarnowski, J. Kåla, A. Kyster, I. Meyer, J. Mogensen, and P. Szyman. 2019. Safe information exchange on board of the ship. TransNav 13 (1): 165–171. https://doi.org/10.12716/1001.13.01.17.

Allianz. 2020. Safety and Shipping Review [Annual report]. Allianz Global Corporate and Speciality. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2020.pdf

Ali, Y., M.A. Awan, M. Bilal, J. Khan, A. Petrillo, and A.A. Khan. 2019. Risk assessment of China-Pakistan fiber optic project (CPFOP) in the light of multi-criteria decision making (MCDM). Advanced Engineering Informatics 40: 36–45.

Alop, A. 2019. The main challenges and barriers to the successful "smart shipping." TransNav 13 (3): 521–528. https://doi.org/10.12716/1001.13.03.05.

American Club. 2020. The Guidelines on Cyber Security Onboard Ships v4 (p. 64). https://www.american-club.com/files/files/Guidelines_on_Cyber_Security_Onboard_Ships_v4.pdf

Androjna, A., T. Brcko, I. Pavic, and H. Greidanus. 2020. Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering 8 (10): 776.

Balduzzi, M., K. Wihoit, and A. Pasta. 2013. Hey captain, where's your ship? Attacking vessel tracking systems for fun and profit. Hack in the Box (HITB) Security Conference in Asia.

Bolbot, V., G. Theotokatos, E. Boulougouris, and D. Vassalos. 2020. A novel cyber-risk assessment method for ship systems. Safety Science 131: 104908. https://doi.org/10.1016/j.ssci.2020.104908.

Bothur, D., G. Zheng, and C. Valli. 2017. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. pp 81–87

Chang, C.H., S. Wenming, Z. Wei, P. Changki, and C.A. Kontovas. 2019. Evaluating cybersecurity risks in the maritime industry: a literature review. Proceedings of the International Association of Maritime Universities (IAMU) Conference

Chauvin, C., S. Lardjane, G. Morel, J.-P. Clostermann, and B. Langard. 2013. Human and organisational factors in maritime accidents: analysis of collisions at sea using the HFACS. Accident Analysis &amp; Prevention 59: 26–37. https://doi.org/10.1016/j.aap.2013.05.006.

CyberKeel. 2014. Maritime Cyber-Risks (p. 26). https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

CYBOK. 2019. The cyber security body of knowledge, V1.0, 31 October 2019. https://www.cybok.or

David, M. 2017. World's First Autonomous Ship to Launch in 2018. Fortune. https://fortune.com/2017/07/22/first-autonomous-ship-yara-birkeland/

Delice, E.K., and G.F. Can. 2020. A new approach for ergonomic risk assessment integrating KEMIRA, best–worst and MCDM methods. Soft Computing 24 (19): 15093–15110.

DNV-GL. 2016. Cyber security resilience management for ships and mobile offshore units in operation. https://www.dnv.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html

DNV-GL. 2018. Class guideline—autonomous and remotely operated ships. DNV GL. http://rules.dnvgl.com/docs/pdf/dnvgl/cg/2018-09/dnvgl-cg-0264.pdf

DNV. 2019. How cyber risk fits into the ISM Code—Industry insights. DNV GL. https://www.dnv.com/expert-story/DigitalMagazineDefault

Dyryavyy, Y. (2015). Preparing for cyber battleships—electronic chart display and information system security. NCC Group. https://www.nccgroup.com/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/

Emovon, I., R.A. Norman, J.M. Alan, and K. Pazouki. 2015. An integrated multicriteria decision making methodology using compromise solution methods for prioritising risk of marine machinery systems. Ocean Engineering 105: 92–103.

European Union. 2020. Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic (No. 13626/20). https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf

Felski, A., and K. Zwolak. 2020. The ocean-going autonomous ship-Challenges and threats. Journal of Marine Science and Engineering 8(1): 41.

Fenrich, K. 2008. Securing your control system: the “CIA triad” is a widely used benchmark for evaluating information system security effectiveness. Power Engineering 112(2): 44–49.

Gallagher, S. 2015. Navy re-ups with Microsoft for more Windows XP support. Ars Technica. https://arstechnica.com/information-technology/2015/06/navy-re-ups-with-microsoft-for-more-windows-xp-support/

Gilks, W. R., S. Richardson, and D. Spiegelhalter. 1995. Markov chain Monte Carlo in practice. CRC Press.

GPS World. 2016. Make it real: Developing a test framework for PNT systems and devices. https://www.gpsworld.com/make-it-real-developing-a-test-framework-for-pnt-systems-anddevices/

Groll, E. 2017. U.S. navy investigating if destroyer crash was caused by cyberattack—foreign policy. https://foreignpolicy.com/2017/09/14/u-s-navy-investigating-if-destroyer-crash-was-caused-by-cyberattack/

Gronholt-Pedersen, J. 2017. Maersk says global IT breakdown caused by cyber attack. Reuters. https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

Heffner, K., and Ø.J. Rødseth. 2019. Enabling technologies for maritime autonomous surface ships. Journal of Physics 1357 (1): 012021.

IAPH. 2021. IAPH cybersecurity guidelines for ports and port facilities, Version 1.0, International Association of Ports and Harbors & World Port Sustanability Program (WPSP), 83 p.

IMO. 2017. Guidelines on maritime cyber risk management, International Maritime Organization, MSC-FAL.1/Circ.3, 5

Jones, K.D., K. Tam, and M. Papadaki. 2016. Threats and impacts in maritime cyber security.

Jozi, S.A., M.T. Shoshtary, and A.R.K. Zadeh. 2015. Environmental risk assessment of dams in construction phase using a multi-criteria decision-making (MCDM) method. Human and Ecological Risk Assessment 21 (1): 1–16.

Kaliszewski, A., A. Kozlowski, J., Dąbrowski, and H. Klimek. 2021. LinkedIn survey reveals competitiveness factors of container terminals: forwarders’ view. Transport Policy 106: 131–140.

Kardakova, M., I. Shipunov, A. Nyrkov, and T. Knysh. 2020. Cyber security on sea transport. Advances in Intelligent Systems and Computing 982: 481–490. https://doi.org/10.1007/978-3-030-19756-8_46.

Kavallieratos, G., V. Diamantopoulou, and S.K. Katsikas. 2020a. Shipping 40: Security requirements for the cyber-enabled ship. IEEE Transactions on Industrial Informatics 16 (10): 6617–6625. https://doi.org/10.1109/TII.2020.2976840.

Kavallieratos, G., S. Katsikas, and V. Gkioulos. 2019. Cyber-attacks against the autonomous ship. In Computer security, ed. S.K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Antón, S. Gritzalis, J. Mylopoulos, and C. Kalloniatis, 20–36. New York: Springer International Publishing.

Kavallieratos, G., S. Katsikas, and V. Gkioulos. 2020b. SafeSec Tropos: joint security and safety requirements elicitation. Computer Standards &amp; Interfaces 70: 103429. https://doi.org/10.1016/j.csi.2020.103429.

Kou, G., Y. Peng, and G. Wang. 2014. Evaluation of clustering algorithms for financial risk analysis using MCDM methods. Information Sciences 275: 1–12.

Lars, J. 2021. Maritime Cyber Security: It's all about the money. Improsec | Improving Security. http://improsec.com/cyber-blog/maritime-cyber-security-its-all-about-the-money

Lee, J.D., and T.F. Sanquist. 1996. Maritime Automation. In Automation and human performance: theory and applications, ed. R. Parasuraman and M. Mouloua, 365–384. Washington, DC: Lawrence Erlbaum.

Lloyd's Register. 2017. Design code for unmanned marine systems. Febrero.

Maritime UK. 2018. Maritime Autonomous Surface Ships—UK Code of Practice. https://www.maritimeuk.org/media-centre/publications/maritime-autonomous-surface-ships-uk-code-practice/

Mohammadi, M., and J. Rezaei. 2020. Bayesian best–worst method: a probabilistic group decision making model. Omega 96: 102075.

Munim, Z.H., O. Duru, E., and Hirata. 2021. Rise, fall, and recovery of blockchains in the maritime technology space. Journal of Marine Science and Engineering, 9(3), 266.

OECD. 2021. Ocean shipping and shipbuilding. https://www.oecd.org/ocean/topics/ocean-shipping/

Plummer, M. 2004. Jags: Just another gibbs sampler.

Rezaei, J. 2015. Best–worst multi-criteria decision-making method. Omega 53: 49–57. https://doi.org/10.1016/j.omega.2014.11.009.

Schmidt, D., K. Radke, S. Camtepe, E. Foo, and M. Ren. 2016. A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Computing Surveys (CSUR) 48 (4): 1–31.

Sen, R. 2016. Cyber and information threats to seaports and ships. In Maritime security: An introduction (2nd edn., pp. 281–302). Elsevier.

Senarak, C. 2020. Port cybersecurity and threat: a structural model for prevention and policy development. The Asian Journal of Shipping and Logistics. 37 (1): 20–36.

Silveira, P., A.P. Teixeira, J.R. Figueira, and C.G. Soares. 2021. A multicriteria outranking approach for ship collision risk assessment. Reliability Engineering &amp; System Safety 24: 107789.

Samonas, S. and D. Coss. 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3), 21–45.

Svilicic, B., I. Rudan, A. Jugović, and D. Zec. 2019. A study on cyber security threats in a shipboard integrated navigational system. Journal of Marine Science and Engineering 7 (10): 364.

Tam, K., and K. Jones. 2018. Cyber-risk assessment for autonomous ships. In: 2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018. Doi: https://doi.org/10.1109/CyberSecPODS.2018.8560690

Thombre, S., M.Z.H. Bhuiyan, P. Eliardsson, B. Gabrielsson, M. Pattinson, M. Dumville, D. Fryganiotis, S. Hill, V. Manikundalam, M. Pölöskey, H. Kuusniemi. 2018. GNSS threat monitoring and reporting: Past, present, and a proposed future. The Journal of Navigation 71 (3): 513–529.

Wang, Y.-M., and T.M. Elhag. 2006. Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment. Expert Systems with Applications 31 (2): 309–319.

Wei Zhe, T. 2017. BW Group computers hit by cyber attack in July. Lloyd's List. https://lloydslist.maritimeintelligence.informa.com/LL111889/BW-Group-computers-hit-by-cyber-attack-in-July

Wróbel, K., J. Montewka, and P. Kujala. 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliability Engineering &amp; System Safety 165: 155–169. https://doi.org/10.1016/j.ress.2017.03.029.

Zaccone, R. 2021. COLREG-compliant optimal path planning for real-time guidance and control of autonomous ships. 22

Zavadskas, E.K., Z. Turskis, and S. Kildienė. 2014. State of art surveys of overviews on MCDM/MADM methods. Technological and Economic Development of Economy 20 (1): 165–179.