# Network Security Risk Analysis of Ship Intelligent Navigation

Yu Zang[1,2](✉), Wen Liu[1,2], Shikai Sun[2], Mingzhi Shi[2], Ming Li[3], and Xiaoyong Kang[1]

[1] China Transport Telecommunications and Information Center, Beijing, China
zangyu@bjtu.edu.com

[2] National Engineering Laboratory of Transportation Safety and Emergency Informatics, Beijing, China

[3] China Ship Research and Development Academy, Beijing, China

**Abstract.** The intelligent ship is drawing increasing attention with its advantages of safety, reliability, energy-saving, environmental protection, and economic efficiency. Compared with traditional ships, the intelligent ship is manifested based on autonomous situational perception, risk identification, and intelligent decision-making functions. The realization of these functions depend on the support of an efficient, reliable, and stable ship-to-shore communication network. Therefore, network security risk analysis of intelligent ship navigation becomes critical. This paper comprehensively analyzed the intelligent ship navigation network security attacks and risks. Firstly, the intelligent ship and some typical schemes such as Advanced Autonomous Waterborne Applications (AAWA) were introduced, and the technical framework and functional modules of intelligent ship navigation were presented. Then the network security requirements from system potential threats and external malicious attacks were analyzed, four security risks including damage, misdirection, obfuscation, and denial of service were classified. Meanwhile, a risk analysis model to quantify the risks from different modules was envisaged and a case study was carried to verify this model. Finally, we drew some interesting conclusions and prospects.

**Keywords:** Intelligent ship · Ship intelligent navigation · Cyber-attack · Risk analysis · Potential threats

## 1 Introduction

In recent years, intelligent ships incorporate new technologies such as modern information and artificial intelligence, which own outstanding characteristics such as safety, reliability, energy-saving, environmental protection, and economic efficiency [1]. They are extensively applied in maritime transportation, ocean research, maritime rights protection, and military fields [2], which become the key direction of the future ship researches. Aiming to improve the safety of marine operations and reduce consumption of ship fuel, countries around the world are actively carrying out research on related technologies and accelerating the transformation of the role of the crew on board. In the future, drivers

L. C. Jain et al. (Eds.): ICWCA 2021, SIST 307, pp. 41–50, 2022.
https://doi.org/10.1007/978-981-19-3486-5_5

working in shore-based control centers can remotely control multiple remote ships at the same time. In the meantime, each ship can automatically perceives the ship's status and surrounding environment, make a certain degree of navigation decision, timely upload relevant information to the shore-based control center, and obtain relevant support information from the shore-based as needed. Therefore, compared with traditional ships, the intelligent ships are mainly manifested in the intelligent navigation function based on autonomous situational perception, risk identification, and intelligent decision-making techniques. Ship-to-shore communication networks support the future development of intelligent ships in the direction of autonomy and unmanned [3]. Hence, intelligent ship navigation poses a higher challenge to network security risk management and control. Nowadays, cyber security incidents in the shipping industry are increasing [4]. In 2015, the London Shipowners' P&I Association announced that the number of ship online frauds is increasing, including intercepting the mail of ship agents, hacking their email accounts to implement plans to replace the original payment account with a new bank account. In 2017 and 2018, Petya's cyber virus hit the world, as a result, the IT systems of many well-known shipping companies' offices and some business units around the world failed and suffered heavy losses. There is a research gap to analyze and monitor the network security risk of ship intelligent navigation. This paper comprehensively analyzes the research status of the ship intelligent navigation network security attacks and risks, the organization is as follows: Sect. 2 introduced the intelligent ship and some typical schemes such as AAWA and presented the technical framework and modules of ship intelligent navigation. Section 3 analyzed the network security requirements from system potential threats and external malicious attacks, 4 security risks including damage, misdirect, obfuscate, and Denial of Service (DoS) were classified. Section 4 envisaged a risk analysis model to qualify the risks from different modules mentioned in Sect. 3. Section 5 drew the conclusion and prospects.

## 2 Background

Intelligent ships apply multiple techniques such as sensors, communications, and the internet of things. Specifically, seven techniques including information perception, communication and navigation, energy efficiency control, route plan, condition monitoring, and fault diagnosis, intelligent navigation are connected in the intelligent integration platform [5–10].

Ship intelligent navigation is to use perception, communication, network information, big data, and artificial intelligence techniques to represent the eyes, ears, brain, hands, and mouth of the pilot. According to the technological evolution of intelligent navigation, International Maritime Organization (IMO) divides the level of autonomy of intelligent ships into four levels, level 1 means seafarers are on board with automated processes and decision support, level 2 means seafarers are on board and ships can be remotely controlled, level 3 means ships can be remotely controlled but the seafarer is not on the ship, level 4 means fully autonomous ship. There are three kinds of typical scenarios for intelligent navigation, remote driving, automatic berthing, and unberthing, autonomous navigation. The technical framework of intelligent ship can be found in Ref [11].

The core of the ship is the intelligent navigation system, it automatically plans the route according to the navigation task firstly. Then situation awareness system is applied to detect the surrounding targets during the route execution. After the target is found, the collision avoidance decision module generates safe collision avoidance, meanwhile, this module continuously verifies the ship's state and evaluates the current control mode. Once the problem is found, and the intelligent navigation system cannot process it. The alarm information is uploaded promptly to the shore-based control center through the data link, the shore-based control center will take over the ship. During the entire process of the route execution, the shore-based control center can remotely monitor the ship's state and location, environment, and the ship through the data link, so that a single control center can monitor and control multiple intelligent ships.

## 3 Network Security Requirements

The network security issues of ship intelligent navigation contain two categories, one is to maintain the integrity and availability of information and systems to ensure business continuity and the continuous use of the system. The other is to prevent hackers from accessing systems and information, to avoid the loss of confidential information and control. Therefore, the analysis of ship intelligent navigation network security requirements is mainly carried out from two aspects. One is the system potential network threats generated by the system's design, and the other is the external malicious attack that the system may suffer.

### 3.1 System Potential Threats

In Sect. 2, the functional modules are presented in ship intelligent navigation, including route planning, situation awareness, collision avoidance decision, state definition, data link, and remote control.

**Route Planning**

(1) Tampering of the current location, mainly comes from the positioning system, such as Global Navigation Satellite System (GNSS) deception. (2) Invalidation of current position, mainly comes from the positioning system, such as GNSS interference. (3) Tampering of destination location, mainly comes from data tampering. (4) False risk information on the route ahead, for example, receiving false Navigational Telex (NAVTEX) navigation warning information, air guidance services, chart correction information, etc.

**Situation Awareness**

(1) Falsification of the electronic nautical chart, for example, if the modified map data is tampered with, such as the water depth value is maliciously increased, the underwater obstruction is maliciously deleted, etc. (2) False targets of Automatic Identification System (AIS), for example, adding a virtual aid to navigation in front of the route will cause the intelligent navigation system to be induced by false targets. (3) Tampering of the AIS data, which cause the ship to misroute, and bring risks to the subsequent route execution risk and action. (4) The false target of ship radar, false radar targets will

likely lead to errors in module, which in turn will bring risks to route execution and collision avoidance operations. (5) Tampering of anemometer data, which brings risks to the ship's maneuvering, especially the ship's entrance and exit ports, berthing, and departure ports. (6) Tampering of the log data, the tampered log data will cause serious accidents such as the ship colliding with the dock.

### Collision Avoidance Decision

(1) Falsification of parameters such as collision risk assessment, which will lead to delays in avoiding collisions, wrong decisions, and serious consequences such as urgent situations, urgent dangers, and collision accidents. (2) Falsification of ship maneuverability assessment data, which will lead to misjudgment of the ship maneuverability.

### State Definition

(1) Tampering of intelligent navigation state data, for example, the state definition module always believes that the ship is in a safe state and does not need to be taken over by remote control. (2) Tampering of Voyage Data Recorder (VDR) data, for example hiding traces of attacks, and affecting accident investigation.

### Data Communication

(1) Functional failure: the route planning module, situation awareness module, collision avoidance decision module, and state definition module cannot obtain various information from sensors, and the modules cannot exchange data. (2) Data is collected viciously: the data transmitted between ship and shore, ship and ship was collected viciously, causing data leakage, and ship dynamic data such as ship location, voyage plan, ship states, and other information were stolen. (3) Data transmission is unavailable: ship-to-shore data transmission is unavailable, which means that the ship cannot report distress alarms and business data to the shore-based control center, and cannot obtain instructions from the shore-based control center, causing the intelligent ship to lose connection and control.

### Remote Control

(1) Tampering of the remote monitoring command, which will cause the intelligent ship cannot execute the route according to the expected target, and the tampering of the key parameters of safe navigation will cause serious collisions, groundings, and other accidents. (2) The remote-control function denies service. The control commands issued by the remote-control system cannot be accurately received and executed by the ship-side intelligent navigation system. (3) An unauthorized third party obtains remote control authority. Third-party attackers obtained control of the ship through illegal attacks, resulting in the hijacking of the ship.

The above potential threats can be classified into 4 categories including damage, misdirect, obfuscate, and DoS. In the route planning module, tampering of the current location, tampering of a destination location, and false risk information on the route ahead belong to obfuscation and misdirect, invalidation of current position belongs to damage. In the situation awareness module, falsification of the electronic nautical chart, tampering of the AIS data, tampering of anemometer data, and tampering of the log data belong to obfuscation and misdirect, false targets of AIS and false target of ship radar belong to obfuscation. In collision avoidance decisions, falsification of parameters such as collision risk assessment and falsification of ship maneuverability assessment data belong to misdirect. In state definition, tampering of intelligent navigation state data and tampering of VDR data belong to obfuscation and misdirect. In the data communication system, functional failure belongs to damage, data is collected viciously and data transmission is unavailable belong to damage and DoS. In the remote control system, tampering of the remote monitoring command belongs to obfuscation and misdirect, the remote-control function denies service belongs to DoS, an unauthorized third party obtains remote control authority belongs to misdirect.

## 3.2 External Malicious Attack

Section 3.1 analyzes the potential threats of the system from the perspective of the system's structure and business design. This section analyzes the network security requirements from the perspective of external physical attacks that the system may suffer. The attack motives of different attackers were explored, including attack cost and attack reward, to determine the security requirements of the ship intelligent navigation.

### Attack Cost

Attack cost means the cost that the attacker must pay when the system is attacked. When determining the cost of an attack, personnel and environmental factors play an important role. For example, the experience and awareness of personnel can prevent or allow cyber-attacks to occur. In addition, the ship's configuration (such as firewalls) and physical location may also determine the likelihood of an attack. For example, In the areas with frequent pirates will mean an attack advantage at these coordinates. If data theft is the target of an attacker, certain ports and networks with weak anti-virus capabilities will increase the risk of being attacked. This paper applies a five-layer structure based on traditional computing systems to indicate the level of "hacking ability" and the available resources required for utilization, more details can be found in Ref [12].

### Attack Reward

In addition to the attack cost, attack rewards are also a factor when executing an attack. To fully understand the psychological factors of cyber attackers, it is necessary to deeply analyze the types of hackers and their motivations. BIMCO divides the cyber attackers in the existing standard security environment into 5 categories including activists, competitors, criminals, terrorists, elitists.

Activists are also called "hacktivists", the ideal goal of radical groups is to achieve ideological influence. Their attack actions contain disrupt activities, disclose information to change the targeted behavior. Although these actions are not offensive, their activities may create opportunities to benefit other attackers or cause accidental damage or leakage. Competitors mean competing companies, and even opposing countries, who may apply cybercrime to increase their market influence in the global economy. In most non-extreme situations, the expected goal is to obtain information. In addition, it is also an incentive to interfere with competitors' ship operations to damage their financial status or reputation. Criminals can range from individuals to groups of different sizes and levels of complexity. Most criminals hope to profit from material theft, fraud, smuggling, and extortion. Simple cyber-attacks can obtain the direct economic benefit, meanwhile, it is organized to sell network tools to all types of attackers to obtain indirect economic benefits. Terrorists' attack purposes are always to seek casualties and property damage. In a more sophisticated attack, the ship may become an asset for a long-range cyber-attack. Elitism always invades the system to test or show off their abilities, such attacks rarely show negative results and are not considered in this paper.

# 4 Network Security Risk Analysis

## 4.1 Risk Analysis Model

Section 3.1 analyzed the potential threats and external attacks from different modules in ship intelligent navigation. This section tries to build the risk analysis model for identified threats and attacks. A two-dimensional quadrant risk analysis framework was applied to quantify the threats and attacks. Tam [12] investigated a model-based method to provide a comprehensive analysis of maritime cyber-risks and the risks can be displayed in 2D and 3D projections separately, the case studies were carried based on the physical structure includes the GNSS, electronic chart display and information system, automatic identification system, etc. For example, misdirection and damage are risks from GNSS. Compared with that, this paper adopted the method proposed by Tam to analyze the risks from different functional scenarios, new ideas are listed as follows: (1) network security risks were analyzed when the ship is navigating from the technical/situational perspective. (2) system potential threats were discussed from the route planning, situation awareness and other functional scenarios. For example, GNSS deception and receiving false NAVTEX navigation warning information both belong to the risks from route planning functional scenario. (3) this research is oriented by the intelligent navigation functional scenarios, which can complement the research conducted by Tam, and finally provide advice on the safety of the ship's intelligent navigation network.

$\boldsymbol{axis_s}$, $\boldsymbol{axis_e}$, and $\boldsymbol{axis_r}$ represent the potential threats, attack cost, and attack reward. Two variables $\boldsymbol{Attacker_a}$ and $\boldsymbol{Target_t}$ are considered to model an attack. The attributes of these two variables are shown in Eqs. (1) and (2).

$$\boldsymbol{Attacker_a} = (a_{vector}, a_{goal}, a_{type}, a_{resources}) \tag{1}$$

$$\boldsymbol{Target_t} = (t_{vulnerabilities}, t_{effects}, t_{type}, t_{resources}) \tag{2}$$

For $\boldsymbol{Attacker_a}$, there are 4 variables. $a_{vector}$ means the attack object such as vulnerable web application, $a_{goal}$ means attackers' expected results such as stolen information and physical collision. $a_{type}$ means the type of attackers. $a_{resources}$ means the ways for attackers to acquire skills, time, money, and members. For$\boldsymbol{Target_t}$, there are 4 variables too. $t_{vulnerabilities}$ means the system vulnerabilities such as outdated operation system or firewall. $t_{effects}$ indicates the possible impact such as loss of navigation after exploiting the vulnerability. $t_{type}$ means the object type such as ferry. $t_{resources}$ represents experienced crew, anti-virus, and other factors that can stop or catch attackers. These 8 variables are not independent of each other. Attackers will decide the $a_{vector}$ according to the$t_{vulnerabilities}$. Combination of $a_{goal}$ and $t_{effects}$ can determine whether an attack succeeds. Four variables such as $a_{type}$, $a_{resources}$ and $t_{type}$, $t_{resources}$ should be considered simultaneously, then an attack can be evaluated accurately. Two-dimensional quadrant risk analysis is to model the function between the $\boldsymbol{Attacker_a}$, $\boldsymbol{Target_t}$ and $\boldsymbol{axis_s}$, $\boldsymbol{axis_e}$, $\boldsymbol{axis_r}$, which is shown in Eqs. (3) and (4).

$$axis_s = f_{vulnerability}(a_{vector}, t_{vulnerabilities}, t_{effects}) \tag{3}$$

$$axis_e = f_{ease}(a_{type}, t_{type}, a_{resources}, t_{resources}) \tag{4}$$

$$axis_r = f_{reward}(a_{type}, t_{type}, a_{goal}, t_{effects}) \tag{5}$$

Based on Eqs. (3), (4), and (5), an action with attacker and target can be quantified from three aspects $\boldsymbol{axis_s}$, $\boldsymbol{axis_e}$, $\boldsymbol{axis_r}$ also means vulnerability $f_{vulnerability}$, ease $f_{ease}$, and rewards $f_{reward}$. The projection formula is shown in Eq. (6)

$$\begin{aligned} F_{action}(attacker, target) &= \mathrm{I}(axis_s, axis_e, axis_r) \\ &= \mathrm{I}(f_v(a,t), f_e(a,t), f_r(a,t)) \end{aligned} \tag{6}$$

Each vulnerability in different modules in ship intelligent navigation can be modeled by ease and rewards as shown in Fig. 1.

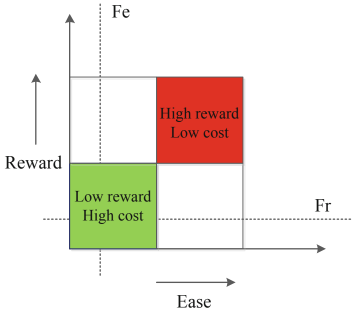

**Fig. 1.** 2-D mapping of risk quadrant for ship intelligent navigation.

In Fig. 1, each risk can be projected to a 2D risk quadrant, evaluators compare the risks of various systems numerically, and they can also consider a series of factors such as attacker types, goals, and effects. The risk also can be assessed by the distance between the data point and the origin. Figure 2 characterized the risk by quadrant to which the vulnerability is mapped. Vulnerabilities in the first quadrant have a high risk because the attackers can get rich rewards for the lower cost. Vulnerabilities in the third quadrant have a low risk because the attacker has the higher cost but the lower reward. If the analysts only own limited resources to mitigate the threat, then filters Fe and Fr can be introduced to filter out the risks that have low rewards but a high-cost investment. In this way, security efforts can be focused on the most likely network security risks.

### 4.2 Network Attack Analysis Based on Risk Analysis Model

Based on the risk analysis model constructed in Sect. 4.1, when all variables in $\boldsymbol{Attacker_a}$, $\boldsymbol{Target_t}$ are fully considered, the two-dimensional quadrant risk model will become too complicated for effective and comprehensive evaluation. Therefore, this paper specifies 2 $\boldsymbol{Target_t}$ variables and 4 $\boldsymbol{Attacker_a}$ variables. In Sect. 3.1, four potential threats are concluded from different modules in ship intelligent navigation include damage, misdirect, obfuscate, and DoS. Experts from ship intelligent navigation score the potential risks for attackers contain activists, competitors, criminals, and terrorists, and different modules, all the data is shown in Table 1.

**Table 1.** Scores of potential risks for different attackers and modules.

| Module | Risk | $H_r$ | $H_e$ | $Co_r$ | $Co_e$ | $Cr_r$ | $Cr_e$ | $T_r$ | $T_e$ |
|---|---|---|---|---|---|---|---|---|---|
| Route planning | Damage | 2 | 4 | 3 | 3 | 4 | 2 | 4 | 2 |
| | Misdirect | 2 | 3 | 3 | 3 | 5 | 3 | 5 | 3 |
| | Obfuscate | 1 | 4 | 3 | 3 | 4 | 3 | 4 | 2 |
| Situation awareness | Misdirect | 2 | 3 | 3 | 2 | 4 | 2 | 4 | 2 |
| | Obfuscate | 2 | 4 | 3 | 3 | 3 | 3 | 3 | 3 |
| Collision avoidance decision | Misdirect | 3 | 3 | 4 | 2 | 5 | 3 | 5 | 2 |
| State definition | Misdirect | 2 | 3 | 4 | 2 | 4 | 2 | 4 | 3 |
| | Obfuscate | 1 | 4 | 3 | 3 | 3 | 3 | 3 | 3 |
| Data communication | DoS | 2 | 3 | 3 | 4 | 4 | 2 | 3 | 4 |
| | Damage | 3 | 3 | 3 | 3 | 4 | 2 | 4 | 3 |
| Remote control | DoS | 2 | 3 | 3 | 3 | 4 | 2 | 4 | 2 |
| | Misdirect | 3 | 2 | 4 | 2 | 5 | 1 | 5 | 1 |
| | Obfuscate | 2 | 2 | 3 | 3 | 5 | 2 | 5 | 1 |

According to Table 1, different projection views can be calculated to visualize the cyber risk of ship intelligent navigation. Evaluation based on the two-dimensional quadrant risk analysis method is not for a risk assessment of a single module, but a summary of the risks associated with each consequence to determine the most likely outcome of a cyber-attack. Figure 2 shows the risk analysis results of the ship intelligent navigation based on the two-dimensional quadrant risk analysis method.

Figure 2 shows the risk identification for different attackers. For all attackers, the DoS and damage belong to the low-reward and high-cost area, which is low risk. For activists, misdirect is in the high-reward and low-cost area, which is high-risk, obfuscate is in the high-reward and high-cost area, which is a great reward for the attacker, but it requires more cost. For competitors, misdirect and obfuscate have the same reward, but the cost of misdirect is lower. For criminals, the rewards for misdirect and obfuscate are roughly the same, but the cost of obfuscate is lower. For terrorists, misdirect can take advantage of

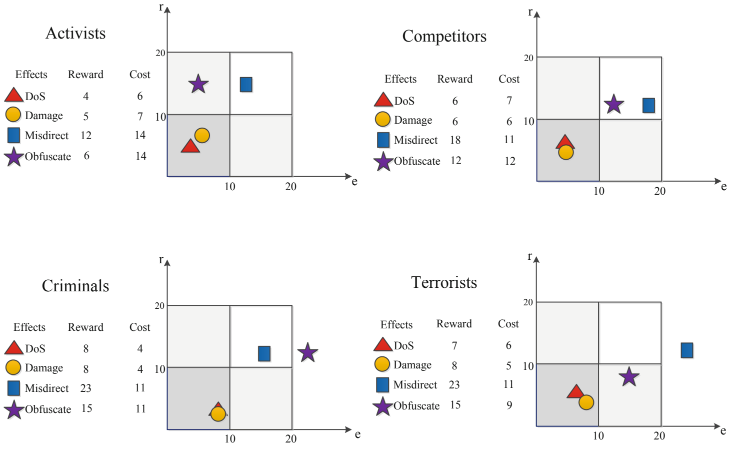

**Fig. 2.** Summary of risks focused on effects.

lower costs to obtain higher rewards, while obfuscate requires additional cost investment, and there is no way to obtain the same return as the misdirect. In summary, for the four types of attackers, the misdirect and the obfuscate are both high-risk threats.

## 5 Conclusion

Compared with conventional network security analysis methods, this paper focused on the unique risks that arise in the process of traditional ship navigation networks and intelligence. First, we comprehensively analyzed the current research status of ship intelligent navigation network security, including intelligent ship technology and various typical intelligent ship solutions, intelligent navigation technology, and its typical functional modules. Then we analyzed the security requirements of the ship intelligent navigation network for each typical functional module, designed a two-dimensional quadrant risk analysis method to quantitatively analyze the network attack and risk of the ship intelligent navigation system, including risk analysis model construction and network attack analysis. Finally, the high-risk threats of ship intelligent navigation networks were determined and concluded, which can provide the theoretical guidance for actual on-site operations.

However, there are few limitations, only two variables are applied in the two-dimensional quadrant risk analysis method, 2 target variables, and 4 attacker variables. So, the risk cannot be fully depicted. In the future, all variables in target and attacker should be considered or selected according to scenarios.

**Acknowledgment.** The paper is financially supported by National Key R&D Program of China (2018YFB1601500, 2018YFB1601504).

## References

1. Li, Y.: Research status and development trend of intelligent ships. Int. Core J. Eng. **5**(11), 49–57 (2019)
2. Yang, T.: Intelligent ships. In: Mukherjee, P.K., Mejia, M.Q., Xu, J. (eds.) Maritime Law in Motion. WSMA, vol. 8, pp. 703–711. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-31749-2_34
3. Guanghang, W., Fenghao, S., Xianbo, X.: Unmanned boat design for challenges and verification of unmanned surface ship intelligent navigation. In: IEEE 8th International Conference on Underwater System Technology: Theory and Applications (USYS), pp. 1–5. IEEE, Wuhan (2018)
4. CNSS Homepage. https://www.cnss.com.cn/html/sdbd/20191012/331834.html. Accessed 02 Dec 2021
5. RØ, J.: The MUNIN project: assessing the feasibility of unmanned ships. Naval Archit. (JAN.SUPPL.), 45–47 (2016)
6. Acanfora, M., Luca, F.D.: An experimental investigation on the dynamic response of a damaged ship with a realistic arrangement of the flooded compartment. Appl. Ocean Res. **69**, 191–204 (2017)
7. VesselFinder Homepage. https://www.vesselfinder.com/vessels/SVITZER-HERMOD-IMO-9788124-MMSI-219022265. Accessed 02 Dec 2021
8. FinFerries Homepage. https://www.finferries.fi/en/news/press-releases/finferries-falco-worlds-first-fully-autonomous-ferry.html. Accessed 02 Dec 2021
9. KONGSBERG Homepage. https://www.kongsberg.com/maritime/about-us/news-and-media/news-archive/2020/first-adaptive-transit-on-bastofosen-vi/. Accessed 02 Dec 2021
10. Anderson, M.: Bon voyage for the autonomous ship mayflower. IEEE Spectr. **57**(1), 36–39 (2020)
11. Rolls-Royce Homepage. https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/%20customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf. Accessed 02 Dec 2021
12. Tam, K., Jones, K.: MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J. Marit. Aff. **18**(1), 129–163 (2019). https://doi.org/10.1007/s13437-019-00162-2