Cyber Security Issues in Implementing Shipping Traffic Separation Scheme (TSS) In Straits of Malacca and Singapore

Chomariyah[1]
Universitas Hang Tuah, Surabaya, Indonesia

Abstract
Owing to the density of the traffic in the Straits of Malacca and Singapore (SOMS), the Traffic Separation Scheme (TSS) did succeed to implement a governance principle between Malaysia, Indonesia and Singapore, the three surrounding nations around SOMS), but there still remained several navigational challenges and threats to maritime such as cybersecurity issues, navigation theft and other types of cybercrimes. This study employed an explorative research design, and made use of documentation research method for data collection. This study unearthed several layers of the cyber and information security domain known as maritime cybersecurity and explored various types of cyber security issues that might prevent the smooth functioning of Traffic Separation Schemes and other shipping communication networks in the SOMS region. This study fulfills the long felt need of examining the existing provisions of regulatory frameworks and the vulnerabilities of e-navigation in the TSS and assessing the cyber security of shipping activities in the Malacca straits. While investigating the landscape of cyber threats amidst actual incidents in the maritime sector, this study forewarns the shipping companies against cyber risks and threats. It also recommends how cybersecurity could be improved in the maritime sector over time, and hopefully it might inspire further research work.

Keywords: IMO, e-navigation, cyber risk, cyber security, shipping communication

Introduction
Straits of Malacca and Singapore (SOMS) stretch over approx. 520 miles from northernmost point of Sumatra to Southern extremity of Goh Puket and 43 miles from Southeast point of Johore to Northeastern extreme of Bintan. The Malacca Strait has experienced a highly dense ship traffic, with annual traffic over 60,000 vessels. The increased traffic due to international shipping has posed significant risks even to the biodiversity and the marine environment, the livelihood of the coastal communities, and the fishing and tourism industries. Owing to the density of the traffic, several navigation aids have been devised to cope up with the competing marine activities and various types of threats to

[1] Department of Law, Faculty of Law, Universitas Hang Tuah, Surabaya 60111, Indonesia. E-mail: chomariyah@hangtuah.ac.id

maritime including the security issues, and navigation theft amounting often to cybercrimes as well. Strategically, this was a high-risk area for navigation because collisions were a major security problem in many sea ports (Ramin et al., 2020; Rasdi et al., 2021).

In 1971, Traffic Separation Schemes (TSS) were introduced for the first time. In a joint Statement, the TSS was adopted as a common governance principle between Malaysia, Indonesia, and Singapore, the three surrounding nations around Straits of Malacca and Singapore (SOMS). Rule 10 of TSS emphasized upon the safety of navigation and declared internationalization of straits as a separate issue. It meant that the governments of Indonesia, Malaysia and Singapore agreed that the SOMS were not international straits, but they could be used fully for international shipping in accordance with the principle of innocent passage. Rule 10 also stated that the three States bordering the Straits should take the primary responsibility about the safety of navigation, environmental protection, and maritime security. To comply with this regulation, a Tripartite Technical Experts Group (TTEG) was established in1975 with Indonesia, Malaysia, and Singapore to discuss the issues related to the SOMS and enhance the experience of international navigation. This step was seen as a good initiative by the three littoral states and their commitment towards ensuring navigational safety, protecting the marine environment, and facilitating the shipping traffic. The tripartite group was consistent with the international law as stayed in the Article 43 of United Nations Convention on the Law of the Sea (George, 2008; Merdekawati et al., 2021; Ozer & Akbas, 2020).

The TTEG comprised maritime experts from the three littoral States. Till date, the TTEG has taken several initiatives to enhance navigational safety and protection of the marine environment in the Straits of Malacca and Singapore (Hashim et al., 2020). One key initiative was the Routing System which enhanced the Traffic Separation Scheme (TSS) and overhauled the shipping traffic rules in the Straits. Another major initiative taken by the TTEG in 1998 was the mandatory ship reporting system (or STRAITREP) in the Straits. The STRAITREP empowered the coastal authorities to update transiting ships on the traffic situation and to contribute positively towards search and rescue response and operations to marine incidents in the Straits. Figure 1 presents its vast extent.

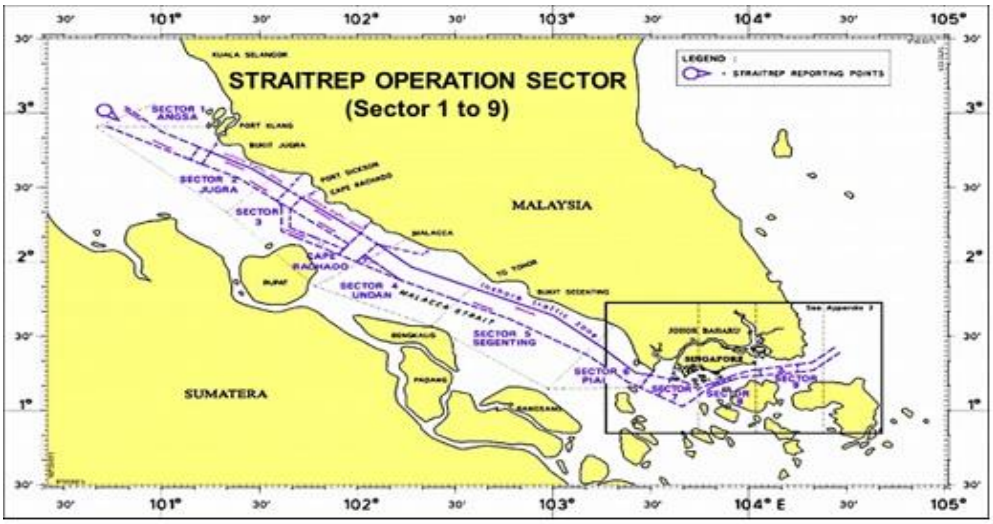

Figure 1: STRAITREP Operating sector
Source: Official website of Marine Department Malaysia,
https://www.marine.gov.my/jlm/page/traffic-separation-scheme

With the implementation of the STRAITREP, the three littoral states developed a co-operative mechanism on safety of navigation and environmental protection in the Straits of Malacca and Singapore. They jointly facilitated user states and other key stakeholders on issues of navigational safety and marine environment protection inside and outside the Straits to ensure a safe international navigation. This not only enhanced the navigational safety of the marine environment but also reduced the risk of marine incidents in the Straits of Malacca and Singapore (Hashim et al., 2020; Leifer, 1978). The tripartite group also initiated to work with a cooperative mechanism to maintain the sovereign rights, jurisdiction and territorial integrity of the littoral States over the SOMS. For this purpose, it outlined the topics such as navigational safety as well as e-navigation by devising a new ship traffic management system and making use of electronic nautical charts and building marine electronic highways for safe data transfer and cope up with navigational hazards (Rusli, 2020; M. Zaman et al., 2021; M. B. Zaman, 2019; Zulkifli et al., 2020). Figure 2 illustrates the Traffic Separation Scheme in the Straits of Malacca and Singapore.

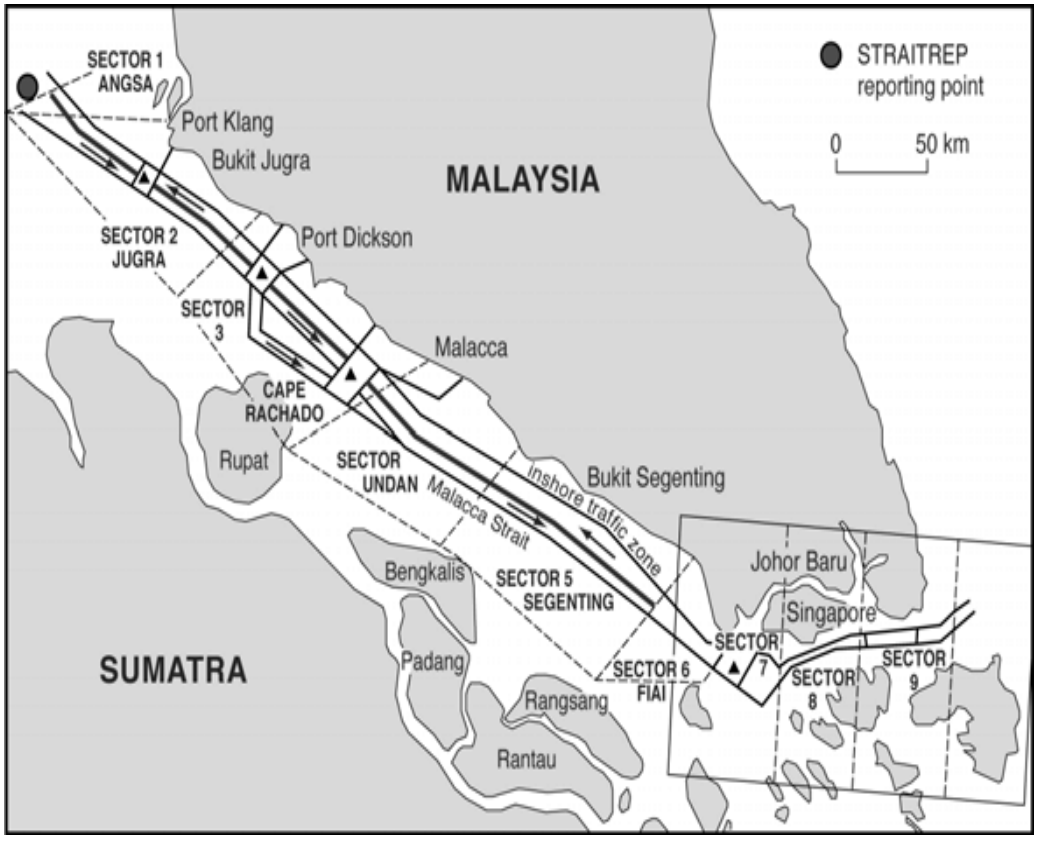

Figure 2: The Traffic Separation Scheme in the Straits of Malacca and Singapore

In more recent times, the shipping safety issues have been redefined. The safety of the navigation data against cybercrime is now seen much more significant to check the pollution of the marine environment or check vessel collisions. Marine traffic analysis reflects that the actual condition of ship navigation is performed to enhance maritime traffic safety. An examination of frauds and crimes such as navigation data theft and piracy committed in the Malacca Strait suggest over hauling of the current security measures and taking revolutionary steps to face the challenges (Hidayat & Tan, 2021).

There are various initiatives already taken to ensure the safety of navigation data. Two of these measures are the use of accurate navigation charts and automatic identification system (AIS) which allow for the accurate investigation of shipping routing and their encounters. Navigations charts are now outdated since they were first used in 1950s and were based on obsolete hydrographic surveys carried out in other straits in UK and the Netherlands and also did not have unified standard (Mak, 2006; Rimmer & Lee, 2007). On the other hand, AIS is the technology-assisted ship navigation systems managed through the ship radars. The AIS provides real time information about ships and their locations through very high frequencies (VHF). The information that AIS transmits between ships and from the ship to the coast or vice versa helps improve their safety and facilitate communication and real time information. The AIS provides information like ship's identity, its types, its speed, MMSI, destination, current location, COG and so on. AIS displays all this information on a chart plotter, or a PC assisted with a marine navigation software (Boyes & Isbell, 2017).

The International Maritime Organization (IMO) is the United Nations specialized agency responsible for stipulating rules, regulations, criteria and guidelines for the safety and security of shipping and prevention of marine and navigation theft. the International Maritime Organization (IMO), as the main United Nations (UN) body to ensure maritime safety and marine environmental protection, plays a central role in adopting codes and recommendations to regulate maritime traffic in both national and international waters [10]. Under the Safety of Life at Sea (SOLAS) convention (regulation V/19.2.4), the IMO mandates the use of AIS on all larger vessels (>300 GT) and all passenger vessels sailing in international waters, in order to make a remote assessment of ship's position, speed and heading, but also compliance with conservation measures (Favier & Fontana, 2020; Jensen, 2015).

In the wake of the pandemic, the IMO also mandated all shipping companies and crew members to configure cyber risk management and safety management protocols ships in their ship safety manuals in accordance with the International Safety Management Code (ISM Code) and strictly adhere to them. During the COVID-19 pandemic, an increase in cyber-attacks was seen against ships and superyachts. During the last one decade, cyber-attacks in the maritime sector increased over 40% annually (BIMCO, 2020); however during the pandemic, cyber-crime increased by more than 400%, as estimated. This suggests the vulnerability of the information technology setups on ships and yachts and failure of operational technology. The increase in the risk curve also suggests that the criminals found more opportunities to attack the cyber systems and put the privacy of all ship owners, yacht crews, and shore-side service providers under risk. The severity of this risk increases when such criminal activity extend to issues such as espionage, damage to reputation, safety of individuals and of vessels, hijacking, ransom and, in worst case, assassination.

In order to develop a defence mechanism, the IMO was forced to issue new guidelines such as installing cyber security systems and practising robust risk management with effect from January 2021. The cyber security of ships across straits globally was also pushed under International Safety Management System (ISM) Codes, vice IMO Resolution MSC.428(98). The new guidelines proposed all ship-owners and managers to periodically assess cyber risk and adopt suitable preventive measures such as using new technology, better autonomy, antivirus enabling, updated versions of software and greater work stability. All these measures should be initiated with a proactive approach, anticipating every possible threat that might come in the form of a cyber-attack (Duke & Osim, 2020; Payne & Hadzhidimova, 2020; Svilicic et al., 2019).

All commercial vessels of more than 500 gross tons were required to comply with new IMO requirements with immediate effect (January 2021). As an extra backup plan, each vessel's cyber security resilience was also linked with the ISM Code, requiring the ship's all cyber arrangements to be configured into its safety management systems and in accordance with the IMO's new regulations. Likewise, coastal authorities were also instructed to increase cyber surveillance

Problem statement

Prior to the introduction of ISM, the jurisdiction of IMO was limited. Article 4 had directed SOMS to work only within the designated sea lanes and implement TSS. When IMO started its operations, one of the measures was to ensure the adherence to the international shipping regulations by all the littoral states and operate within their respective jurisdictions. However, whenever a need was felt to amend the international rules, the littoral states would make proposals before the IMO, which would be discussed and approved in mutual interest. For instance, in 2005, Indonesia and Malaysia demanded separating security issues from the issues of navigation safety when the Indonesia-Singapore Coordinated Patrols failed to tackle piracy issues and sea robbery threats. Lloyd's Joint War Risks Committee had also listed the SOMS region as "high-risk war zone" (Zulkifli et al., 2020).

Currently, there are pressures from the domestic administrations of the three littoral states. It is evident that a distrust has developed between the three littoral states on security issues and there does not exist any efficient bilateral or tri-lateral framework. The entire global shipping industry is demanding to "internationalize" the issue of SOMS's security (M. Zaman et al., 2021; M. B. Zaman, 2019; Zulkifli et al., 2020). The safety issues are so grievous that demands are made to take the help from Chinese/Japanese/Indian patrolling vessels to escort each commercial vessel passing through SOMS to safe zones. The security concerns have grown more post 9/11 and US has proposed a Regional Maritime Security Initiative (RMSI) and a unified Malacca Strait Patrol (MSP) service. Eventually, in 2005, a coordinated patrol titled Malacca Straits Sea Patrol (MALSINDO) was launched jointly by Indonesia, Malaysia and Singapore (M. Zaman et al., 2021; M. B. Zaman, 2019).

In the meantime, cyber threats and online risks have also endangered the security of the navigation data, but very few initiatives have been taken to check this threat (Bellamy, 2020). In 2006, a combined maritime air patrol agency called Eyes-in-the-Sky (EiS) was launched with the assistance of Thailand. A Malacca Straits Patrol Joint Co-ordinating Committee was also formed which made members sign Terms of Reference and Standard Operating Procedures for e-navigation for the Malacca Straits Patrolling. In 2008, the Intelligence Exchange Group (IEG) was launched to enhance the Malacca Straits Patrol Information System (MSP-IS) in order to consolidate information-sharing, data protection and checking against hacking and cyber threats. In 2009, Singapore Navy hosted the Information Fusion Center (IFC) to act as a regional maritime security center and facilitate information sharing, coordination and collaboration through the use of e-navigation technology. Despite all these initiatives, there is still a need to launch a robust anti-cybercrime intelligence system or bring changes in the current operations to check all types of security threats.

The paper is organized as follows: The first part dealt with the background information about the current state of safety mechanisms employed in the SOMS and a problem statement of the current study. The next section discusses significant findings of the study

highlighting types of maritime based attacks, vulnerabilities in shipping sector, regulatory framework and cybercrimes in shipping industry. The third section presents an analysis of the cybersecurity landscape in the maritime sector and finally, the last section, conclusion, provides some recommendations.

Findings

i. *Types of Maritime-based cyberattacks*

Cybercrimes in shipping industry are not much different from what exist at any other places. There can be data hijacks, hacking attacks, phishing, dangerous malware and viruses. Initially, the cyber criminals made virus attacks on PCs of the crew and coast officials to hack the documents. These viruses entered into PCs through crew members who loaded pirated computer games on their personal computers and laptops which risked both their data and the machines. Since PCs are isolated devices, the virus would remain limited and not spread to the system computers. However, in modern times of digitalization of data and internet operations, a cyberattack would be more dangerous and problematic and carry a more malicious intent (Miranda Silgado, 2018; Tam & Jones, 2019).

Due to digitalization and online operations, ships are required to be integrated with coast side operations to smoothly conduct business, manage operations, and maintain communication with the headquarters. A few of these operations are critical to the safety of navigation and carry out a few legitimate functions such as monitoring engine performance, maintenance of spare parts, loading and unloading of cargo, power and energy management and stow planning during and post voyage. These operations produce a lot of data which may be exploited by cyber criminals to indulge in maritime-based cyberattacks and cause business disruption and subvert the supply chain in several ways. They may compromise equipment and machines, or software and supporting services to be delivered to / from the ship. their main aim is to damage the reputation or defame the shipping company that may be held guilty of breaching the International Ship and Port Facility Security Code (ISPS Code) and its noncompliance caused due to the delay of the vessel.

Often the hackers may indulge in espionage and steal sensitive information and sell it to the competitors. The shipping businesses also sometimes are victims of distributed denial of service (DDoS) attacks, a hacking event that takes control of multiple computers and prevents legitimate and authorized users from accessing information or usually by flooding a network with data. For their vested interests, the attackers may also manipulate passenger lists, indulge in illegal activities, breach sensitive cargo transports, cause engines failures, shut down vessels, or even disrupt the onboard control systems (Caponi & Belmont, 2015). The attackers may also demand extortion/ransomware from the ships to restore operations digital piracy by shutting down the vessel/port. Such malicious attacks on ships could sometimes debilitate the whole operating system, preventing cargo bookings, delaying cargo documents and stopping or de-routing payments of dues and invoices (Zăgan et al., 2018).

ii. *Vulnerabilities in shipping sector*

The increase in cybercrime in the recent years has made the shipping sector more vulnerable. Owing to these vulnerabilities, new types of crimes such as cyber espionage supply chain subversions, cyber activism, and cyber terrorism have crept in the maritime domain. A typical rise in spear-phishing of vessels at sea has also been discovered. An example of this vulnerability was presented in a BIMCO survey which showed how a malicious software (malware) can significantly degrade the functionality of the ship's onboard computer system, thus making an impact on its control system. The BIMCO

survey also showed how the maritime companies suffered huge losses of their systems and work practices but were also exposed to risk across their supply chain (BIMCO, 2020). The results of the survey hinted at the vulnerability of the shipping company toward cybercrime. Several studies have identified the vulnerability of a ship's onboard systems to a cyberattack (DiRenzo et al., 2015; Hareide et al., 2018; Tam et al., 2016). A few have highlighted the weaknesses of these systems and the failure of modern technologies and the integrated IT (Information Technology) and OT (Operational Technology) networking and internet connectivity.

Owing to such vulnerability, anonymous hackers succeed in disrupting ships' communications system and steal sensitive information. They can easily penetrate into the OT system of the shipping company and get the remote access to intelligence systems through the satellite and breach the 4G, or Wi-Fi connections of the vessel (Glomsvoll & Bonenberg, 2017). Technological vulnerability thus expose the lack of data integrity and lack of alignment of the onboard systems with the cyber safety and cyber security measures, remotely available at the headquarters of the shipping company. This could have very dangerous consequences including a targeted attack to their databases and accounting information.

Two empirical studies (Svilicic et al., 2019) and (Hareide et al., 2018) demonstrate that integrated navigational systems (INS), are more vulnerable to cyberattacks. Though a disconnection from the internet might prevent outside threats but vulnerabilities could still arise from the offline operating system triggered by a crew member unintentionally or maliciously. Likewise, the BIMCO survey (CyberSail, 2016) found the positioning systems (GPS, AIS, Radar), Electronic Chart Display and Information System (ECDIS) engine control, and monitoring are most vulnerable systems onboard ships. The reason is that AIS and GPS are not encrypted or authenticated, and hence they are potentially vulnerable to cyberattack. ECDIS is so vulnerable that it is much easier for a cybercriminal to modify its files and infect the INS with malicious content (Hareide et al., 2018), resulting in directing the vessel to a false route or position. A few examples include a cyberattack that misdirected two naval ships to a false route in 2016 in the Persian Gulf. A year later, in February 2017, a German-owned 8250 TEU container vessel fell victim to cyber-criminals who deactivated its navigation system. The Voyage Data Recorder (VDR) is also a good example of cyberspace vulnerability as it is connected to the ship's systems that are linked to online services through satellite communications (Kala & Balakrishnan, 2019).

iii.Regulatory Framework and organizations

The SOMS falls within the scope of international navigation regulations in accordance with Article 37 and Article 38 of the IMO, which concerns the right of transit passage enjoyed by all ships and aircrafts. The states bordering a strait are under an obligation not to hamper transit passage and there shall be no suspension of transit passage under Article 44 (Proelß, 2017). There are two significant regulatory documents issued by the IMO. First is the IMO's resolution (MSC.428(98), 2017) on Maritime Cyber Risk Management mandating every shipping company to get Safety Management System (SMS) approved prior to its operations (IMO, 2017b). The resolution insisted that the approved SMS should be built upon the objectives and functional requirements of the International Safety Management Code (ISM Code) (ISM, 2018). Second, the IMO has developed certain guidelines on maritime cyber risk management in the form of recommendations to safeguard ships from cyber threats and vulnerabilities (IMO, 2017a).

Aligned with both IMO documents, there is a third regulation known as "Guidelines on Cyber Security Onboard Ships," which provides practical recommendations on maritime cyber risk management, covering both cybersecurity and cyber safety. In addition, IMO is also preparing, in collaboration with the International Electro-technical Commission (IEC), a new standard for maritime navigation and radio-communication equipment and systems: IEC 63,154 "Cybersecurity—General Requirements, Methods of Testing and Required Test Results" (International Electrotechnical Commission, 2019). The US has specifically taken the initiative and established the Information Sharing and Analysis Centres (ISACs) to act as "trusted entities" and guide the shipping industry against physical and cyber threats and their mitigation (European Union Agency for Cybersecurity, 2018). A second US agency, known as Information Sharing and Analysis Organization (ISAO), is also actively working to implement the US government regulations and helping the shipping industry to fight cyber threat. Likewise, in the EU, the organization known as The European Cyber Security Organization (ECSO) set up a cybersecurity Contractual Public–Private Partnership (cPPP) cell to legal and ethical support to the maritime sector against cybercrimes.

In 2019, the EU Cybersecurity Act was established with new objectives and tasks to implement cybersecurity in the EU and provide a legal framework to all digital products, services, and processes (European Union, 2017). Specifically for the maritime sector, there already exists the 2014 European Union Maritime Security Strategy which recognizes cyber as one of the risks in the maritime domain (Council of the EU, 2014, 2018; European Commission, 2020a, 2020b; European Union Agency for Cybersecurity et al., 2019). Recently, the EU also devised a Security Union Strategy for 2020–2025 (European Commission, 2020a) against cyberattacks and cybercrimes by calling upon community approach to security and unitedly fight the risks to infrastructures in transport and maritime sectors.

iv. Cybercrimes in shipping industry

The shipping sector refrained from publicizing cyber-attacks until 2017 when AP Møller Maersk, the largest Danish international shipping and logistics company, made public the NotPetya malware attack on its computer system, which caused the company a loss of over $300m in revenue. After this cyber incident infected the IT systems of the shipping giant Maersk, it was forced to shut down all its operational devices and handle all operations manually (Hareide et al., 2018; Lagouvardou, 2018; ShipInsight, 2018). There are two other major cyber incidents reported in 2018. The first occurred when COSCO Shipping Lines fell victim to a cyberattack. The company's internet connection was disrupted within its offices in the Americas. After activation of COSCO's contingency plans, operations were back to normal after five days. Being aware of what happened to Maersk, they had taken proactive steps to minimize their risk of a cyberattack.

The second incident occurred in October 2018 when the Australia-based ferry and defense shipbuilder Austal was hit by a cyberattack that penetrated their data management systems. The attackers managed to steal internal data and offered some of it for sale on the dark web in an apparent extortion attempt. Carnival Corporation was the latest to fall victim to a ransomware attack on its IT systems in August 2020. The cybercriminals managed to download certain data files related to guests and employees' personal data, which could result in potential claims from guests, employees, shareholders, or regulatory agencies. Besides, there are several leading liner operators and logistics companies that were subjected to malicious activities such as phishing e-mails and hacking on a daily basis putting their data at high risk.

Various guidelines have been given to tackle cyber security in the shipping industry such as those by IMO, BIMCO, Class societies, P&I club and others (Cimpean et al., 2011) For instance, the IMO released a document called MSC-FAL.1/Circ.3 Guidelines recommending high level action plan and functional elements to achieve maritime cyber risk management. The MSC adopted the Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems for bringing effective maritime cyber risk management. The BIMCO Guidelines are the most comprehensive ones as these are based on inputs from at least 16 shipping companies. Last, but not the least, guidelines of the class societies are customized upon class notation data of vessels which employed best practices.

Discussion

Article 41 of IMO recommended setting up sea lanes along the straits to be governed by traffic separation schemes (TSS). The proposal contained a mandatory ship reporting system in the Straits of Malacca and Singapore known as STRAITREP, which IMO's Maritime Safety Committee (MSC69) approved on 1 December 1998. The provisions of STRAITREP followed the mandate of the International Convention for Safety of Life at Sea (SOLAS), which emphasized on navigational safety, navigation efficiency and protection of marine environment. The STRAITREP was applicable on all ships plying the Straits of Malacca and Singapore (SOMS). All ships regardless of length were required to maintain instant communication with other ships, and the coastal authorities through their Very High Frequency (VHF) Marine Radio fitted with radiotelephony services. The STRAITREP facilitated transferring and receiving communication and particularly distress signals between ships in the periphery and coastal authorities. The coastal authorities would advise ships about the traffic situation in the Straits and paths of safe transition in case of a search-and-rescue (SAR) operation and to avoid marine hazards.

The SOMS was also the first Strait to implement United Nations Convention on the Law of the Sea (UNCLOS). It was also the first strait to implement the IMO Art.43 which required all littoral states to demonstrate their willingness to cooperate with the user states and other stakeholders. This showed that the three littoral states, Indonesia, Malaysia and Singapore, recognized each other's sovereignty, sovereign rights and jurisdiction over the waters of the SOMS. This can be seen as adherence to the international law. However, despite this sovereignty, the vulnerability of the shipping industry to cyberattacks was still evident in the inevitable use of technology and software based systems and instruments. The dependence on e-navigation for all types of operations further increased the risk of cyber-attacks. In an attempt to check cyber-attacks, certain regulations were framed. Initiatives such as integrated navigation systems and mandatory use of Electronic Chart Display and Information System (ECDIS)and VDR data were adopted to check the cybercrimes. The ECDIS is a type of geographical information system introduced by IMO as an alternative to paper nautical charts employed in nautical navigation. Both ECDIS and VDR could prevent the contamination of the system to some extent.

However, a drawback was felt when neither IMO nor any other international regulatory agency mandated any basic safety training under SOLAS or Standards of Training, Certification, and Watchkeeping (STCW) for seafarers or crew members working onboard commercial ships or superyachts. If this could take place, there would be enough trained staff to prevent cybercrimes or contribute to system recovery in case of contingent situations. However, operations under Global Maritime Distress and Safety System (GMDSS) or under International

Ship and Port Facility Security Code (ISPS), a few safety norms could be implemented to enhance maritime security and by complying with the ISM guidelines and compliance to implement through the International Convention for the Safety of Life at Sea (SOLAS).

It has also been felt that cyberattacks take place when a large range of IT equipment such as personal computers, laptops, tablet devices, servers, networking routers, switch gears, sensors, actuators, radar are used in excess (Jensen, 2015). With the advent of advanced technology, when ships switch over to automated control systems and e-navigation for performing complex functions, there is a great change not only in the cost reduction and performance improvement but also in checking the cybersecurity-related risks (Babineau et al., 2012; Masala & Tsetsos, 2016). However, cyber criminals show their ability to infiltrate into satellite navigation, especially the GPS and jam the operating systems through malwares like denial of data reception (competing signals) or spoofing (false signals) (Glomsvoll & Bonenberg, 2017). The IMO introduced the Automatic Identification System (AIS) for navigation safety and to protect the satellite navigation applied on ships and ports but that too was cracked by hackers (DiRenzo et al., 2015; Ziebold et al., 2016).

Cyber security strategies need to take into account targets and reasons for attack and vulnerabilities of the system. Financial gain or competition could be the cause of most cybercrimes, shipping companies with large operational networks would be on top priority of the cyber criminals. The cybercrimes are mostly in the form of attacks on coastal networks in order to cause disruption to services and endanger the shipping networks and systems. The role of shipping companies and owners is very crucial here. Unless they take the onus to protect their own sensitive information and commercial assets, the safety and security of ports is also jeopardized. Often the training to crew members or seafarers would not work as hackers and cybercriminals are steps ahead of the equipment manufacturers and system designers. For instance, ECDIS or VDR data could easily be infected by a virus by inserting a memory stick into a personal device connected to it.

In the shipping industry, the communication systems and equipment surveillance are the most vulnerable points that could be under cyberattacks. The communication system checks the shipping traffic and the equipment monitor their movement and the crew officers working on that system. Though there might be firewalls and virus protection but unless these protected gears are regularly updated, the system can be easily infected with indigenized viruses. Moreover, it is difficult to maintain a constant surveillance on emails and data exchanges since the crew might open an attachment to an e-mail without even imagining that it could be a malware targeting to attack their communication system. The question is whether to stop all types of such crew communication if the problem of cybercrime continues to grow in such a manner. It is also difficult to monitor the equipment as the anti-viruses cannot constantly scan the communication system for the corrupt data or detect the communication system has been compromised.

IMO has undoubtedly redefined navigation regulatory framework and extended its jurisdiction to maritime safety and security through e-navigation. It made positioning, navigation, and timing (PNT) services more robust and cybercrime-safe by introducing a more viable terrestrial system called LOng-RAnge Navigation (LORAN) or eLoran which is capable to provide not only better horizontal positioning accuracy to prevent the damage or disruption to the maritime transportation system (MTS) (Radgowski & Tiongson, 2014) but can also pre-warn against cyber-induced environmental attacks that might put the maritime environment at stake.

Conclusion

Despite all preventive cyber protection and cyber security measures, the shipping defense mechanism has failed to check malicious hackers and cyber criminals. Studies have suggested that cyber-criminals employed not only primitive and tailor made hacking tools such as spoofing and phishing or attacking crew-members' emails with malware, but also made use of very advanced maritime enabled tactics which could at least subvert their ship's supply chain and corrupt their communication systems. Analysts have studied both residual risks and software-borne viruses and come to several conclusions including providing training to marine supply chain crew members for detecting cyber-attacks and potential phishing; observing the nature of cyber-attacks and understand their modus operandi; making the supply chain communication more robust and finding measures how to block cyber-attacks by successfully identifying malicious attempts in advance.

There are various other suggestions such as embedding a high level of security networks in shipping communication systems and providing suppliers the remote access to navigation and other OT systems to get backup support on board and, if required, allow suppliers to take over the entire control for upgrading or remote servicing and exterminate any unidentifiable malware placed by hackers. Such shore side and external access points with suppliers or at headquarters should be free from unauthorized access. Other strategies that can work is to segregate the control systems related to cargo stowage, loading and unloading, and disallow any guest access in the form of passenger recreation or private internet access for the crew.

Effectively segregated networks are capable of impeding the cyber attacker's access to the ship's communication systems and prevent the spread of malware. Although remotely piloted and automated marine vessels are revolutionary steps in maritime operations, but these make vessels more vulnerable to cyberattacks. IMO should consider navigation issues and cyber risks while creating rules for autonomous shipping. Last, but not the least, any wireless network onboard should also be discouraged. If required, onboard wireless networks should be partitioned by firewalls to create safe zones. All these measures could help in the prevention of cyber-attacks.

References

Babineau, G. L., Jones, R. A., & Horowitz, B. (2012). A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions. *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 99-104). IEEE. https://doi.org/10.1109/THS.2012.6459832

Bellamy, C. (2020). What are maritime crime and maritime security? *International Journal of Maritime Crime & Security, 1*(1), 13-25. https://news.slpa.lk/wp-content/uploads/2020/06/maritime-paper.pdf

BIMCO. (2020). Safety at Sea and BIMCO publish cyber security white paper. https://www.bimco.org/news/priority-news/20190916-safety-at-sea-and-bimco-publish-cyber-security-white-paper

Boyes, H., & Isbell, R. (2017). *Code of Practice - Cyber Security for Ships.* Institution of Engineering and Technology. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. *Intellectual Property & Technology Law Journal, 27*(1), 16. https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cybersecurity-10-2014.pdf

Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A., & Hellebooge, L. (2011). Analysis of cyber security aspects in the maritime sector. https://trid.trb.org/view/1125656

Council of the EU. (2014). *European Union Maritime Security Strategy. 11205/14.* https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf

Council of the EU. (2018). *Council conclusions on the revision of the European Union Maritime Security Strategy (EUMSS) Action Plan. Annex to 10494/18.* https://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf

CyberSail. (2016). *IHS & BIMCO – Survey Findings.* https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf

DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015). The little-known challenge of maritime cyber security. *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)* (pp. 1-5). IEEE. https://doi.org/10.1109/IISA.2015.7388071

Duke, E. O., & Osim, S. (2020). From festival to social communion: a Nigerian experience. *Przestrzen Spoleczna (Social Space Scientific Journal), 19*(1), 53-69. http://socialspacejournal.eu/Social%20Space%20Journal%2012020(19).pdf#page=53

European Commission. (2020a). *Communication from the Commission on the EU Security Union Strategy.* COM(2020) 605 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605

European Commission. (2020b). *Report on the implementation of the revised EU Maritime Security Strategy Action Plan.* Joint Staff Working Document. https://ec.europa.eu/oceans-and-fisheries/document/download/9d55fef9-d923-43b3-9efd-d927284a1da0_en

European Union. (2017). *JOINT STAFF WORKING DOCUMENT: Second report on the implementation of the EU Maritime Security Strategy Action Plan.* https://data.consilium.europa.eu/doc/document/ST-10398-2017-INIT/en/pdf

European Union Agency for Cybersecurity. (2018). *Information sharing and analysis centres (ISACs) : cooperative models.* European Network and Information Security Agency. https://doi.org/10.2824/549292

European Union Agency for Cybersecurity, Zisi, A., Sarri, A., Drougkas, A., & Kyranoudi, P. (2019). *Port cybersecurity : good practices for cybersecurity in the maritime sector.* European Network and Information Security Agency. https://doi.org/10.2824/328515

Favier, J., & Fontana, É. (2020). La blockchain, au service de la sécurité. *Res Militaris, 10*(1), 1-36. https://resmilitaris.net/index.php/2020/01/01/id1031540/

George, M. (2008). *Legal Regime of the Strait of Malacca and Key Benefits.* LexisNexis.

Glomsvoll, O., & Bonenberg, L. K. (2017). GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation, 70*(1), 33-48. https://doi.org/10.1017/S0373463316000473

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *The Journal of Navigation, 71*(5), 1025-1039. https://doi.org/10.1017/S0373463318000164

Hashim, N. H. C., Harun, M., Ahmad, M. Z., & Abdullah, W. M. W. (2020). Maritime Territorial Dispute In The Malacca Straits Between Malaysia And Indonesia, With References To Their Bilateral Diplomatic Negotiation Process. *International Journal of e-Navigation and Maritime Economy, 15*, 50-62. http://db.koreascholar.com/article.aspx?code=407183

Hidayat, A., & Tan, J. (2021). *Maritime Security Threats: Issues and Challenges in Malaysia's Maritime Domain*. A Maritime Nation. https://books.google.com/books?id=BZw9EAAAQBAJ

IMO. (2017a). *MSC-FAL.1/Circ.3: GUIDELINES ON MARITIME CYBER RISK MANAGEMENT*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3.pdf

IMO. (2017b). *RESOLUTION MSC.428(98): MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS* https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

International Electrotechnical Commission. (2019). *Maritime Navigation and Radiocommunication Equipment and Systems-Cybersecurity-General Requirements, Methods of Testing and Required Test Results* (Edition 1.0 ed.). IEC 63154 ED1. https://standards.iteh.ai/catalog/standards/iec/49130033-ce6f-488d-bf44-1acd9eb7a6d7/iec-63154-2021

ISM. (2018). *The International Safety Management (ISM) Code*. IMO Publishing. https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

Jensen, L. (2015). Challenges in maritime cyber-resilience. *Technology Innovation Management Review, 5*(4), 35-39. http://doi.org/10.22215/timreview/889

Kala, N., & Balakrishnan, M. (2019). Cyber Preparedness in Maritime Industry. *International Journal of Scientific and Technical Advancements, 5*(2), 19-28. http://ijsta.com/papers/IJSTAV5N2Y19/IJSTAV5N2R1Y19.pdf

Lagouvardou, S. (2018). *Maritime Cyber Security: concepts, problems and models*. [Master Thesis]. Technical University of Denmark. https://backend.orbit.dtu.dk/ws/portalfiles/portal/156025857/Lagouvardou_MScThesis_FINAL.pdf

Leifer, M. (1978). *Malacca, Singapore and Indonesia*. Brill Nijhoff. https://brill.com/view/title/10079

Mak, J. N. (2006). Unilateralism and Regionalism: Working Together and Alone in the Malacca Straits. In O.-W. Graham Gerard (Ed.), *Piracy, Maritime Terrorism and Securing the Malacca Straits* (pp. 134–162). ISEAS Publishing. https://doi.org/10.1355/9789812305909-011

Masala, C., & Tsetsos, K. (2016). A Demanding Challenge for the Maritime Industry. In H.-C. Enge & D. Göge (Eds.), *Look-Out 2016 Maritime Domain Cyber: Risks, Threats & Future Perspectives* (pp. 11–26). Lampe & Schwartze KG. https://elib.dlr.de/98812/1/Look-Out%202016_web.pdf

Merdekawati, A., Ajari, S., Hasibuan, I. A. T., & Agung, I. G. P. (2021). COMPATIBILITY OF INDONESIA'S REGULATIONS ON SUBMARINE CABLE WITH UNCLOS 1982. *Arena Hukum, 14*(2), 293-313. https://doi.org/10.21776/ub.arenahukum.2021.01402.5

Miranda Silgado, D. (2018). *Cyber-attacks: a digital threat reality affecting the maritime industry*. [Dissertations]. World Maritime University. https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations

Ozer, M. M., & Akbas, H. (2020). The Predictability of IQ on Delinquency: A Structural Equation Model (SQM). *International Journal of Criminal Justice Sciences, 15*(2), 283-297. http://dx.doi.org/10.5281/zenodo.4738960

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology, 14*(1), 81-105. http://dx.doi.org/10.5281/zenodo.3741131

Proelß, A. (2017). *United Nations Convention on the Law of the Sea: A Commentary.* Nomos Verlagsgesellschaft. http://dx.doi.org/10.5040/9781472561688

Radgowski, J., & Tiongson, K. (2014). Cyberspace—The Imminent Operational Domain. *Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council, 71*(4), 18-21. http://www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf

Ramin, A., Mustaffa, M., & Ahmad, S. (2020). Prediction of Marine Traffic Density Using Different Time Series Model From AIS data of Port Klang and Straits of Malacca. *Transactions on Maritime Science, 9*(02), 217-223. https://hrcak.srce.hr/249531

Rasdi, N. M. I. B., Russtam, M. I., Suhrab, R. I., Ahmed, T., & Fung, C. L. F. (2021). Safety of Navigation at the Straits of Malacca. *World Wide Journal of Multidisciplinary Research and Development, 7*(10), 1-9. http://wwjmrd.com/archive/2021/10/1660/10.17605/OSF.IO/TNZK7

Rimmer, P. J., & Lee, P. T. (2007). Repercussions of Impeding Shipping in the Malacca and Singapore Straits. *Journal of International Logistics and Trade, 5*(1), 7-26. http://dx.doi.org/10.24006/jilt.2007.5.1.001

Rusli, M. H. M. (2020). Navigational hazards in international maritime chokepoints: A study of the Straits of Malacca and Singapore. *Journal of International Studies, 8*, 47-75. http://www.e-journal.uum.edu.my/index.php/jis/article/view/7926

ShipInsight. (2018). Cybercrime in shipping – the curse of the computer age. https://shipinsight.com/articles/cybercrime-in-shipping-the-curse-of-the-computer-age

Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A study on cyber security threats in a shipboard integrated navigational system. *Journal of Marine Science and Engineering, 7*(10), 1-11. https://doi.org/10.3390/jmse7100364

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs, 18*(1), 129-163. https://doi.org/10.1007/s13437-019-00162-2

Tam, K., Jones, K., & Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. *Engineering & Technology Reference*, 1-12. http://dx.doi.org/10.1049/etr.2015.0123

Zăgan, R., Raicu, G., Hanzu-Pazara, R., & Enache, S. (2018). Realities in maritime domain regarding cyber security concept. *Advanced Engineering Forum. 27* (pp. 221-228). Trans Tech Publications. https://doi.org/10.4028/www.scientific.net/AEF.27.221

Zaman, M., Kobayashi, E., & Zubaydi, A. (2021). Traffic analysis for enhancing safety in the Singapore Straits using AIS data. *IOP Conference Series: Earth and Environmental Science. 649*(1) (pp. 012065). IOP Publishing. https://doi.org/10.1088/1755-1315/649/1/012065

Zaman, M. B. (2019). Navigation Safety for Marine Traffic in the Malacca Strait using AIS Data. *Asian Journal of Applied Sciences, 7*(4), 386-397. https://doi.org/10.24203/ajas.v7i4.5827

Ziebold, R., Romanovas, M., & Gewies, S. (2016). Experimental Evaluation of the Impact of Jamming on Maritime Navigation. *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016)* (pp. 3461-3480). https://doi.org/10.33012/2016.14810

Zulkifli, N., Ibrahim, R. I. R., Rahman, A. A. A., & Yasid, A. F. M. (2020). Maritime cooperation in the Straits of Malacca (2016-2020): challenges and recommend for a new framework. *Asian journal of research in education and social sciences, 2*(2), 10-32. https://myjms.mohe.gov.my/index.php/ajress/article/view/9601/4470