Evaluation of the maritime security threats and issues to the future of the shipping industry – Maritime Autonomous Surface Ships

Tin Long Cheung
City University of London, UK
Maritime Operations and Management

Keywords
Maritime Autonomous Surface Ships (MASS), maritime security, piracy & armed robbery at sea, terrorism, smuggling and trafficking, cyber and hybrid security

Abstract

Nowadays traditional manned commercial sea-going vessels are facing several difficulties, including shipping accidents that are mainly caused by human errors and the shortage of seafarers with the associated increased manning cost. In 2021, the International Maritime Organisation Maritime Safety Committee (IMO MSC) had finished the Regulatory Scoping Exercise (RSE) regarding Maritime Autonomous Surface Ships (MASS) at its 103rd session, taking its first step towards autonomous shipping that does not involve human vectors. This paper analyses the security issues that are potentially involved in fully autonomous ships (Degree Four of Autonomy) (DOA 4) of MASS operations and recommend measures to adjust and mitigate the issues. This paper reviews six conventional maritime security threats that could threaten a DOA 4 vessel, including piracy and armed robbery at sea, terrorism, smuggling and trafficking, stowaways, cyber security threat and hybrid security threat. The research methodology of this paper reviews different literature as the source of both quantitative data and qualitative evidence.

This paper analyses the experience of the security incidents in other comparable sectors and systems in order to identify the characteristics and behaviour of the security threats. Then the information is analysed against the specific characteristics of MASS operations to consider whether the characteristics of MASS operations may become more vulnerable if exploited by perpetrators of security threats. Potential issues and scenarios of the security threats in the operations are also discussed. Risk assessments are applied to explore the risk level of the security threats in DOA 4 MASS. This paper demonstrates that the characteristics of DOA 4 MASS operations may still pose vulnerabilities that can be exploited by all the six security threats. The risk of terrorism, smuggling and trafficking, cyber security, and hybrid security threats are high in DOA 4 MASS operations, while the risk of piracy and armed robbery at sea and stowaways are medium. Both the aspects of cyber security, detection/monitoring equipment, reliability of vessel systems, security in Shore Control Centres (SCC) and security in ports contribute significantly to the security of DOA 4 MASS operations against these security threats.

This paper recommends all the aspects mentioned in the above findings should be considered in the development of future instruments regarding DOA 4 MASS operations. The stakeholders involved in DOA 4 MASS operations should apply any possible cyber security and detection/monitoring measures even beyond the legal requirement. The security and personnel management of SCC should be ensured too. Finally, further research on the identified security threats on DOA 4 MASS operations is recommended once more practical data on the operations are available, further research on different DOA of MASS operations and different security threats are also recommended.

Corresponding author: Tin Long Cheung
Email address for corresponding author: beenobobo1234@gmail.com
First submission received: 21st December 2021

Revised submission received: 15th May 2022
Accepted: 24th August 2022

1. Introduction

In the maritime industry and ship operations, one of the major hazards caused by human error is ship collision. According to Ung (2019), the occurrence of human errors in marine accidents is at an undesired level and around 75% to 96%. Human error, like negligence and over-working can cause misjudgement and mistakes during navigation, resulting in collisions. The consequence of collision can be significant, for example, pollution from oil leakage and the remaining shipwreck can endanger navigation, causing potential loss of life/injury and the shipping company could suffer significant financial and reputational loss.

The United Nations Conference on Trade and Development Review of Maritime Transport (2020), states the volume of international maritime trade had expanded and reached 11.08 billion tons in 2019. The global commercial shipping fleet had also increased to 98,140 commercial ships, equivalent to a capacity of 2.06 billion deadweight tonnage. The growth of the global shipping fleet will result in busier seaways, maritime choke points and ports potentially leading to greater collision risk. In contrast to the growth of the global world fleet, it is expected the supply of seafarers to crew the vessels may not be able to keep pace with the world fleet expansion. The Maritime Executive (2021) stated that it is estimated that the supply of seafarers available to man the vessels in the global commercial fleet will reduce from an average annual growth rate of 2.7% to only 0.5% within five years. Hence, the shipping industry may face potential seafarer shortage leading to increasing crewing costs in the coming years due to the imbalance between the demand for seafarers and the seafarer supply from the labour market.

As the technologies of ship design advance, the introduction of Maritime Autonomous Surface Ships (MASS) autonomous navigation systems may potentially reduce the requirement for crews to navigate and conduct watchkeeping operations and could even enable ships to operate without any crew, resolving the issues mentioned above.

The International Maritime Organisation (IMO) Maritime Safety Committee (MSC) completed the Regulatory Scoping Exercise (RSE) at its 103rd session recently (IMO, 2021) to respond to the concerns from member states regarding how to regulate MASS. The IMO MSC RSE defined the term MASS as "a ship which, to a varying degree, can operate independently of human interaction". The IMO (2021) further defined the Degree of Autonomy (DOA) as follows:

Degree of Autonomy	Description
DOA 1	Ships with decision support and automated processes. Onboard crews' control and operate shipboard functions and systems. Some operations can be automated and may be unsupervised, however, onboard crews should be ready to take control in case of emergencies.
DOA 2	Ships that can be remotely controlled and operated from another location, for example, on the shoreside. However, onboard crews are available to operate and take control of shipboard functions and systems.
DOA 3	Ships that can be remotely controlled and operated from another location without crews onboard.
DOA 4	Fully autonomous ships which the operating system is able to carry out decisions making tasks, the ship can determine actions by itself.

Table 1. Degree of Autonomy of MASS

The IMO (2021) examined whether MASS could be potentially regulated by the current instruments including International Convention of the Safety of Life at Sea 1974 (SOLAS 1974), The International Ship and Port Facility Security Code (ISPS Code), International Safety Management Code (ISM Code). Multiple potential themes and gaps were identified across several instruments and IMO MSC noted that the best way to address these MASS issues may be to develop a goal-based MASS instrument like "MASS Code" (IMO, 2021).

The IMO MSC RSE is only a starting point to solve the issues of MASS operations. First, the results of IMO MSC RSE do not provide detailed solutions on how to solve and regulate the issues of MASS, they only provide general regulatory directions defining which issues need to be clarified and considered. The IMO MSC RSE mainly reviewed the issues of MASS from a regulatory standpoint in which several instruments were examined to determine whether they can address the issues in their current format. However, the results seem to lack in-depth analysis regarding the potential threats to MASS operations from a security perspective and examine what security threats MASS operations could possibly encounter and their characteristics.

There are maritime security threats that are commonly experienced by traditional manned vessels, including piracy, smuggling and terrorism. Although MASS are subject to autonomous control, they are still being categorised as "ships". Thus, it is logical to assume that MASS may also be vulnerable to the conventional maritime security threats experienced by traditional manned shipping operations. However, due to the characteristic differences between MASS and traditional manned vessels, these security issues may affect MASS differently. It is therefore important to reanalyse the relationship between the characteristics of MASS and these security threats in order to evaluate whether they are still relevant and if there are any vulnerabilities that may specifically pose a threat to MASS operations.

The aim of this paper is to research the security issues MASS operations are vulnerable to, in order to understand the role of different aspects of security studies in the case of MASS operations. The aspiration is to supplement the IMO MSC RSE in the field of maritime security studies and offer some thoughts about potential vulnerabilities that the research has exposed.

2. Methodologies and Limitations

DOA 4 MASS are selected for focused research out of the four DOA MASS. The primary reason for this decision is that systems of DOA 4 MASS have the most distinctive characteristics among all the four DOA of MASS which significantly differentiates them from traditional manned vessels the most. It is the only category that does not have any 'man in the loop'. Therefore, DOA 4 may be the most unique among all the four DOA for security studies of MASS. Another reason is that DOA 4 MASS is the most advanced MASS design in the current stage. The design of the other three DOA of MASS may eventually evolve into or be designed as DOA 4 MASS. Hence, it is believed that DOA 4 MASS has the most research value among all the four DOA of MASS due to its uniqueness and advancement.

The following six areas of security studies that are posed by conventional merchant shipping are selected for focused research in order to further examine the potential of the crimes and the relationship between DOA 4 MASS operations and maritime security threats:

1. Piracy and Armed Robbery at Sea
2. Terrorism
3. Smuggling and Trafficking
4. Stowaways
5. Cyber security threat
6. Hybrid security threat

This paper focuses on only the security of the ship. MASS operations may be categorised into two major operations, first is the port activities such as cargoes loading/unloading, bunkering, berthing. The second is the ship voyage at sea. Hence, the security of MASS operations can be categorised into port security and security of the shipat sea.

During a voyagea ship can berth in different ports in different states which can vary significantly. For example, the geographical characteristics, the degree of automation and utilisation of AI of port facilities, the domestic legislation, the resources of security and law enforcement forces. This is an enormous and complex subject that requires focused research on port security. An attempt to cover multiple ports will significantly exceed the limitation of the scope of work of this paper. Consequently, the scope of research of this paper will focus on the security of ships underway on a voyage only, as the ship security is regulated by international regulations, universal flag states and have similar designs and characteristics. However, general port security issues and recommendations will be discussed, as port security is still undeniably important in MASS operations and, indeed, may be equally, if not even more, important.

Since the development of MASS is still in a very early stage, the usage of MASS by shipping companies is very limited and rare. Therefore, the data relating to security incidents in MASS operations in current commercial shipping environment are limited. The discussion element of this paper relies on analysing the experiences in different comparable sectors and the attempt to predict the potential security threats scenarios when MASS operations become popular, with the assumption of the DOA 4 MASS systems being well developed and matured. Whilst the predictions of this paper may differ from the future practical situation of MASS operations, this paper posits that DOA 4 MASS will be adopted but that systems reliability between the assumption and in practice may vary. Hence, further research on this subject is recommended once more real-life data regarding MASS operations become available

The research methodology comprises a literature review as the source of both qualitative evidence and quantitative data. This paper will be divided into three major sections: discussion, findings, and recommendations.

Under the Discussion section, six sub-sectors represent each of the six areas of security studies. Each sub-sector consists of tables containing the following information:

Investigation of the security incidents in other comparable sectors and systems: In this part, the experiences of security incidents on other comparable sectors and systems will be gathered to analyse the characteristics and behaviour of the security threat, which the understanding of the experiences of security incidents can act as the basis of the investigation of how the security threat may behave in DOA 4 MASS operations.

Analysis of the security threat in MASS operations: This part analyses whether the specific characteristics of MASS operations may become vulnerabilities that can be exploited by the identified behaviours of the security threat, potential issues, and scenarios. The security threat in MASS operations will also be discussed in this sector.

Findings will be put forward and risk assessments will be applied to examine the risk level of the six identified areas of security studies in DOA 4 MASS operations. The observations regarding the operations and security threats such as common aspects that contribute to the security of DOA 4 MASS operations against these threats will also be included.

Relevant recommendations, security measures and mitigations will be suggested to resolve and address the identified six security threats in MASS operations. The types of suggestion may include legal advice and practical measures.

3. Discussion

Kavallieratos, Katsikas and Gkioulos (2019) stated that autonomous ships consist of three major systems:

1) The Engine Automation Systems (EAS) including sub systems like Autonomous Engine Monitoring and Control systems (AEMC) which are responsible for the management and generation of the MASS's propulsion and power systems.

2) The Bridge Automation Systems (BAS) including sub systems like Autonomous Navigation (NAVs) and Ship Controllers systems which are responsible for crucial ship bridge's functions like navigational and management systems.

3) The Shore Control Centre (SCC) including sub systems like Human Machine Interface (HMI) and Remote Maneuvering Support System (RMSS) which enabled SCC to control the MASS.

The coordination between different MASS systems allows her to autonomously perform functions that are crucial to commercial shipping operations, for example, BAS and EAS together can perform navigation and collision avoidance activities, BAS can perform cargo management functions, while SCC enables the communication and control between shoreside and the ship.

The capability of SCC's control allows it to override the decision and automated processes of the MASS systems. For example, SCC remote control overrides the auto navigation by BAS. This paper believes SCC can be placed above all MASS systems in the systems architecture of autonomous ships. An alternative architecture of autonomous ships based on that of Kavallieratos, Katsikas and Gkioulos (2019) is developed and shown in Figure 1 below:

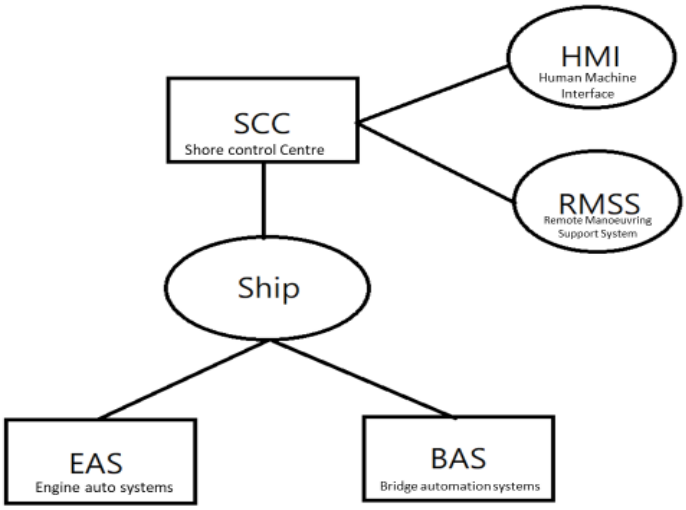

Figure 1. Systems architecture of autonomous ships

The design of DOA 4 MASS, fully autonomous ships will have operating systems that are able to carry out decisions, complete tasks and determine actions without any human interaction. This paper believes the living space for onboard personnel may not be necessary as the DOA 4 MASS commercial shipping operations will not require personnel onboard working and controlling the ship anymore. The physical design and appearance of MASS could potentially be quite different to conventional crewed ships. It is anticipated the MASS vessels would comprise two major structures; the cargo holds and the enclosed space where the systems of MASS are installed, which may be reduced and enclosed like a black

box. The onboard physical control station may also be removed as DOA 4 MASS would not require onboard crew to control the ship. A range of sensors, other than BAS sensors, which are used for navigational purposes. There would probably be basic onboard detection and monitoring equipment like CCTV or even more advanced passive infra-red sensors and potentially drones to allow the SCC to monitor the onboard situation and detect onboard security threats.

The paper believes the SCC should still maintain the role of monitoring and supervising the DOA 4 MASS, in order to prevent or control any unexpected threats. However, details including the ratio of personnel required to manage a number of vessels, as well as the location and activity (entering/leaving port, loading/discharging cargo, navigating vessel choke points – Suez Canal or Panama Canal, or mid-ocean navigation) may heavily depend on different related aspects such as shipping company's policies, protocol, insurance, and legal instruments' requirements, which is unclear at this time.

For MASS operations in ports like cargo loading/unloading operations, the vessel's systems may be able to autonomously carry out cargo loading/unloading operations entirely by herself throughout the voyage (Kavallieratos, Katsikas & Gkioulos, 2020). This paper's author believes that there will be no onsite personnel when the vessel is carrying out operations in Smart Ports. These ports may be equipped with port's equipment such as autonomous vehicles and cargo management systems to allow effective interaction between autonomous ship and port facilities. Some ports are already at an advanced point of testing and adopting these systems including Port of Hamburg, which is using fully automated trucks (ShipInsight, 2021). Also, basic detection and monitoring equipment like CCTV or even more advanced equipment like passive infra-red sensors, scanners and drones may be installed to ensure port security and monitor the operations.

3.1 Piracy and Armed Robbery at sea

Characteristics	Description	Example of past incidents
Hijacking vessels for ransom	Hijack ship and hold crew hostage for ransom, usually keeping the hostage unharmed. Pirates usually attack in a group from their mothership. Pirates will use tools like knotted climbing ropes or ladders to board the ship (BMP 5, 2018). Firearms may be used to threaten the master to stop the ship.	MT Gemini incident: Somali pirates hijacked the ship and held crew's hostage for a ransom of USD 6 million (Mudi, 2011).
Theft of cargoes/ship's stores	Boarding the vessel to steal cargoes or use another vessel to perform ship to ship transfer of the cargoes. Boarding vessels unseen, possibly when the ship is at anchor to steal ship's stores.	Historically common piracy practice in the Gulf of Guinea to transfer refined petroleum products. Common in Bay of Bengal and off SE Asia.
Hijacking vessels for trade	Hijack the ship, get rid of the crew, and sell the cargoes, then disguise the ship as another phantom vessel and use her for trading.	Common piracy practice in the South China Sea.
Variety in funding	Funding in piracy activities can vary. Some pirates may have few resources. However, the involvement of terrorists and organised crime groups may allow pirates to have a much larger scale of impact by using advanced technologies equipment. Piracy can be used to fund terrorism.	Somali pirates originally were fishermen then turned to commit piracy acts in order to earn money to survive (Schneider & Winkler, 2013).

Table 2. Categories of security incidents of piracy & armed robbery at sea in other comparable sectors and systems

Characteristics of MASS	Analysis of threat in MASS operation
No onboard crews and absence of physical control stations	Conventional methods of physical boarding the vessel to hijack the vessel and hold crew members hostage for ransom may not be effective.
Cyber vulnerabilities of MASS systems	Pirates with sufficient resources and technical knowledge may use cyber-attacks and hybrid attacks to hijack or disable the ship. Once the unmanned vessel has been hacked, the vessel may be lost completely as there are no onboard crews to deactivate the external control or shut the power of the systems to stop the vessel (Vinnem and Utne, 2018). The pirates may then extort money from shipping companies by contacting the shipping company for a ransom of the cargoes and vessel with a cost that the shipping company finds commercially more expedient to pay than delay without necessarily declaring the incident.
SCC vulnerabilities	Vulnerabilities of SCC personnel may be targeted by pirates to assist their piracy activities, for example, disabling the MASS systems to allow the pirates to steal cargoes.

Table 3. Analysis of the security threat of piracy and armed robbery at sea in MASS operations

3.2 Terrorism

Characteristics	Description	Example of past incidents
Hijacking vessels	Hijack ship and hold onboard people hostage to achieve their political objective. Using the hijacked vessel as a weapon.	MS Achille Lauro was hijacked by the terrorists and people onboard were being held hostage to pressure the government to release fifty Palestinian prisoners (Liput, 1985). In the aerial transport sector, terrorists hijacked plane to carry out suicide attack against the United States on 11 September 2001.
Use of explosives	Using explosives to cause casualties and damage properties. For the maritime transport sector, vessels are common targets for terrorists, however, ports can be targets too.	The usage of explosives in the MV Superferry 14 incident (Elegant, 2004). The use of explosives in the port city of Mumbai in 2008 (Mirror, 2008).
Cyber attacks	Carrying out cyber-attacks to achieve their political objective.	Cyber-attacks from Syrian Electronic Army in Syria Civil War resulted in a sharp drop in US financial markets (Foster, 2013).
Usually have adequate funding	Terrorists usually have adequate resources and knowledge to conduct terrorist attacks with larger scale and more advanced technologies.	Usage of cyber-attack and various firearms.

Table 4. Categories of security incidents of terrorism in other comparable sectors and systems

Characteristics of MASS	Analysis of threat in MASS operation
Cyber vulnerabilities of MASS and SCC systems	Cyber-attacks can become a powerful force multiplier for the terrorists to carry out terrorist attacks. Terrorist groups with technological expertise and resources to cyber hijack the MASS can turn her into a dangerous weapon. For example, remote control her to ram into the shoreside infrastructures with explosives. There already were cases that terrorists controlled unmanned vessels to carry out ramming terrorist attacks. For

	example, remote-controlled explosive boats were used to ram the Saudi frigate Al Madinah in January 2017 (Olimpio, 2018). As MASS can be a larger vessel like tankers and container ships, the kinetic energy of ramming is much higher (Vinnem and Utne, 2018) and more explosives can be planted on the vessel, resulting in the destruction caused by hijacked MASS terrorist attacks will be significantly larger than small boats. There are also other terrorist attack methods that can be caused by cyber-attacks. For example, using cyber-attacks to control Operational Technology (OT) of the vessel and Information Technology (IT) of the shipping company/government/port. Jamming or hacking the BAS and EAS to sabotage the systems, causing malfunction of rudder and engine, losing control of speed, disabling the systems. Thus, stopping the vessel when she is passing through traffic chock points like Suez Canal to block the path, or making her become a vessel not under command and ram into infrastructure, causing environmental destruction by oil pollution and shipwrecks. Also, using the cyber vulnerabilities between the connection of MASS and SCC to carry out cyber-attacks, stealing critical information and threatening the company or government, disrupting the port activities, etc.
SCC vulnerabilities	Terrorists could hijack MASS if the security measures of SCC are inadequate, for example, SCC personnel are bribed to assist their activities, or the terrorists use firearms to storm the SCC to hijack multiple MASS at once.
Absence or reduced number of port personnel	Fully autonomous ship/port interaction may mean no or fewer onsite personnel to check the situation during port activities such as cargoes loading/unloading and bunkering operations, for example, less port staff to check containers before they are sealed. It is possible that terrorists can secrete explosives into the vessel even the vessel and port are equipped with basic detection/monitoring equipment as they may not be able to cover every spot and corner, especially by terrorist groups that are well organised and have adequate resources. There is a possibility that terrorists may sneak into a port, for example, using jammers to disable detection equipment to evade being detected or target ports with loose security measures, then planting explosives onboard the ship or secreting them into cargoes. Later the ship transports the explosive to a major port, which the explosives explode in a major port without any warning and cause significant casualties and damage to properties.

Table 5. Analysis of the security threat of terrorism in MASS operations

3.3 Smuggling and Trafficking

Characteristics	Description	Example of past incidents
Hidden goods in vessels	Smugglers and traffickers may secrete their goods in various hidden places onboard the vessel. For example, a package of drugs can be hidden within the stow of bulk cargoes onboard a bulk carrier, inside the cargoes of the containers onboard a containership, in the cargoes of cars onboard a Ro-Ro vessel or machinery spaces of the vessels, etc. (Smith, 2020). Besides small items, humans can also be smuggled and trafficked.	20 tons of cocaine worth over $1 billion were hidden in seven shipping containers onboard MSC Gayane on 17 June 2019 (Miller, 2021). 12 tons of cocaine were concealed in a bulk shipment of coal when the Malaysian authorities intercepted the bulk carrier in 2019 (Solum, Åsgård & Urdahl, 2021).
Bribing or disguise as personnel	It is also common for traffickers and smugglers to bribe or target vulnerable crews to assist them to carry the items (Smith, 2020), for example, crews may be bribed to help the criminals to carry contraband and hide it in their personnel belongings. In some cases, although the	Several reports of drug traffickers disguised as port's personnel such as stevedores to assist the trafficking operations since crews cannot inspect the interior

	crews are not involved in the trafficking operations, the crews may have no idea the vessel is being used for trafficking drugs when port staff are involved in the trafficking operations (Smith, 2020).	anymore when the container is sealed and delivered for loading (Solum, Åsgård & Urdahl, 2021).
Usually have adequate funding	Smuggling and trafficking usually involve international organised crime groups (UNODC, 2017) which have adequate technologies and resources.	Smugglers and traffickers have the resources and knowledge to carry out cyber-attacks on ports to smuggle goods undetected (Pasternack, 2013).

Table 6. Categories of security incidents of smuggling and trafficking in other comparable sectors and systems

Characteristics of MASS	Analysis of threat in MASS operation
Cyber vulnerabilities of MASS and smart port systems	Cyber-attacks can help the smugglers and traffickers to gain access to hidden spaces on MASS, for example, hacking deck and cargo machinery systems to gain access and hide items under power winches and cranes (Tam and Jones, 2018). Also, jamming vessel and port detection equipment to evade detection and hacking port facilities to smuggle and traffic goods more efficiently, for example, hacking the database of the port's cargoes management systems to track the movement of the shipping container and steal the containers before the owner arrived (Pasternack, 2013). When the MASS is sailing near the coast, the organised crime groups may hack or use jammers to sabotage the BAS, EAS, and SCC, stopping the vessel, causing signal loss, and disabling onboard detection and monitoring equipment. Then they can carry out their smuggling or trafficking activities when the MASS systems are malfunctioning, for example, performing ship to ship transfer of the cargoes without going through the risk of getting caught by the security checks in ports. When the MASS systems become active again, the criminals may have already finished their activities and escaped.
SCC vulnerabilities	The responsible personnel in SCC may be bribed to assist their activities.
Absence or reduced number of port personnel	The fully autonomous characteristics of MASS operations indicate that there may not be onsite staff around the ship/port interface when carrying out cargo loading/unloading operations, for example, fewer port staff to check containers before they are sealed. Instead, basic detection equipment like CCTV may still exist and people are present in the SCC or remote-control centre to respond to emergencies or monitor the operations. However, Jalonen, Tuominen & Wahlstrom (2017) stated that autonomous vessel's detectability may not be able to fully cover all decks, rooms, and surfaces. Hence, it is still possible that smugglers and traffickers may successfully evade detection and hide their goods, either humans or items in the cargoes and hidden places of MASS during the operations in the ship/port interface even the port and vessel are equipped with basic detection equipment. For example, using divers to attach a "mule" container to the hull of the ship in port which is then detached at the next port.

Table 7. Analysis of the security threat of smuggling & trafficking in MASS operations

3.4 Stowaways

Characteristics	Description	Example of past incidents
Difficult to detect	Stowaways use different methods to board the vessel, for example, bribing the crews or port workers to board the vessel, disguising as crews or stevedores to board the vessel, hiding in containers before they are loaded and climbing up the rudder or stern part of the vessel, etc. Most stowaways are only discovered once	M/T Nave Andromeda incident in October 2020, seven stowaways were discovered on board the tanker when she was crossing the English Channel which they attempted to hijack. (Gardner,

	the ship has set sail (Dryad Global, 2021).	2020).

Table 8. Categories of security incidents of stowaways in other comparable sectors and systems

Characteristics of MASS	Analysis of threat in MASS operation
Absence or reduced number of port personnel	The absence or reduced port and ship staff during port activities may reduce the chance of preventing stowaways if effective detection equipment is missing in the port and vessel. For example, stowaways may be able to avoid the detection of basic detection equipment like CCTV and break into the containers to hide, which there are no onsite personnel to check the condition of containers.
SCC vulnerabilities	SCC personnel may also be bribed to allow the stowaways to secrete onboard the ship.
Absence of crews onboard	There are no onboard crews to immediately handle the onboard situation if the stowaways are detected at sea. Technical issues like lack of accommodation space, food, and freshwater for stowaways, indicates that the characteristics of DOA 4 MASS may not be able to provide immediate humanity treatment to stowaways and are not favouring their activities. Other legal issues like the definition of Master in DOA 4 MASS operations, the SCC personnel responsibilities, the requirement, and condition of the repatriation of stowaways are not clear at this stage, which requires further clarification in the future instruments. It may be more efficient to focus on the prevention of stowaways in ports at the current stage.

Table 9. Analysis of the security threat of stowaways in MASS operations

3.5 Cyber security threat

Characteristics	Description	Example of past incidents
Variety of adversaries	The background, motivation and objective of the attackers can vary, for example, the objective of terrorists and smugglers can be different, resulting in their attack methods also diverging. The scale of cyber-attacks can also vary according to the level of resources of the attacker, for example, an organised crime group may have more funding than an individual hacker.	Drug traffickers recruited hackers to breach the port IT systems that controlled the movement and location of containers to facilitate their international drug trafficking activities in Port of Antwerp (Bateman, 2013).
Variety of attack method	Cyber-attacks can be untargeted cyber-attacks that exploit widespread vulnerabilities on the internet (The Guidelines on Cyber Security Onboard Ships V4, 2020), causing collateral damage to other facilities and organisations. Example of typical tools being used includes malware[1], water holing[2] and typo squatting[3]. They can also be targeted attacks in which the	A.P. Moller Maersk was affected by the collateral damage of an untargeted malware cyber-attack on 27th June 2017 and approximately suffered $300 million loss in revenue (Novet, 2017). The ransomware cyber-attack

[1] Malware is a generic term for a variety of malicious software, which can infect computer systems and impact on their performance.

[2] Water holing is a targeted attack strategy in which cyber criminals compromise websites that are fertile ground for potential victims and wait for the planted malware to end up on their computers.

[3] Typo squatting, also called URL hijacking of fake URL, relies on mistakes such as typos made by internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to an alternative and often malicious website.

	attackers may use techniques and tools that are more complex and specifically created for their targets. Example of typical tools includes denial of service and phishing[4].	on Transnet almost stopped the entire function of the container terminals around the country, which the port officials were required to manually record the movement of the vessels (O'Neill, 2021).
Attack in distance	Cyber-attacks can be carried out in distance, for example, an unauthorised person on the shore can attack a vessel sailing at sea through the internet and signal connection between the satellite and vessel bridge systems.	Distance GPS spoofing attack in Black Sea affected over 20 vessels, which they were not able to obtain GPS signal (Goward, 2017).

Table 10. Categories of security incidents of cyber security threat in other comparable sectors and systems

Characteristics of MASS	Analysis of threat in MASS operation
Cyber vulnerabilities of MASS systems	The systems of DOA 4 MASS may require internet access, exchange of signals and high exposure to the internet to maintain their function, the IT and OT[5] systems of MASS are almost entirely integrated too. The attackers may use different tools like malware to attack these cyber vulnerabilities in the systems to achieve the objectives of denial of service, spoofing, tampering, repudiation, information disclosure and elevation of privilege (Kavallieratos, Katsikas & Gkioulos, 2019). For example, the BAS can be hacked by terrorists by spoofing to hijack the ship and planted explosives to carry out terrorist attacks, or pirates can jam the satellite signal in transit between Human Machine Interface (HMI) and SCC to deny the monitoring of vessels from SCC, thus carrying out ship to ship transfer of cargoes without being detected.
Cyber vulnerabilities of SCC and port systems	For shoreside, the port facilities and SCC require high exposure to the internet and the exchange of satellite and radio signals. SCC mainly carries out the function of ship management and monitoring which requires a certain degree of internet access and exchange of signals even if the operations are fully autonomous. SCC, as a part of commercial shipping company, may also require continuous internet access, the usage of signals like broadband and wireless communication to carry out different daily business functions. Port facilities especially for Smart Ports involve a wide usage of autonomous and digitalised management systems that required a certain degree of internet access and exchange of signals, for example, digitalised vessel traffic management systems and autonomous cranes. Criminals may target these vulnerabilities, for example, sending malware emails to the SCC personnel to hack into the SCC database to steal sensitive and confidential business information for ransom.
Cyber vulnerabilities of third parties	Subverting the supply chain is one of the cyber-attacks techniques that aims to compromise equipment, supporting services or software being delivered to the vessel or company (The Guideline on Cyber Security Onboard Ships V4, 2020). For example, if the e-mail service used by SCC personnel has loose cyber security measures, hackers may be able to steal critical business information of the company through the loophole of the e-mail service provider's server. Another example is the company buying ship or shoreside equipment from third party providers, while the company is unaware of the

[4] Phishing refers to the process of deceiving recipients into sharing sensitive information with a third party.

[5] Information Technology (IT) manages data and support business functions, Operational Technology (OT) is the hardware and software that directly monitors/controls physical devises and processes and as such are an integral part of the ship/port. If IT and OT are integrated this leaves OT systems and processes vulnerable to cyber-attack.

	pre-installed malware or other cyber-attacks software in the equipment systems by hackers.

Table 11. Analysis of the security threat of cyber security in MASS operations

3.6 Hybrid security threat

Characteristics	Description	Examples of past incidents
Variety of adversaries	The background, motivation and objective of the attackers can vary, for example, the objective of pirates and traffickers can be different, resulting in their attack methods also diverging. The scale of hybrid attacks can also vary according to the level of resources of the attacker, for example, an organised terrorist group may carry out hybrid attacks more efficient than an individual attacker.	Four commercial vessels were attacked near Fujairah, United Arab, and Emirates, which their GPS and communication signals were jammed without warning (Satelles, 2019).
Variety of attack method	Hybrid attacks consist of a concerted set of mutually reinforcing threats, for example, the combination of physical attacks and cyber-attacks. It usually involves the usage of physical jamming devices, Electromagnetic Pulse (EMP) weapons or electronic jamming equipment. The jamming occurs when the jammers emit radio signals of the same frequency of the targeted systems, interfering with the systems' signals and disrupting them (Satelles, 2019). The EMP weapons create an electromagnetic field that can short-circuit a wide range of electronic equipment (Washington State Department of Health, 2003). This equipment can be secreted into the cargoes which later load onboard the vessel, the attackers can use a boat to approach the underway vessel to acquire her within the effective range of the equipment, or even carry out the attack from the shore depending on the equipment's effective range.	

Table 12. Categories of security incidents of hybrid security threat in other comparable sectors and systems

Characteristics of MASS	Analysis of threat in MASS operation
Cyber vulnerabilities of MASS systems	The systems of DOA 4 MASS may require internet access, exchange of signals and high exposure to the internet to maintain their function, the IT and OT systems of MASS are almost entirely integrated too. Different adversaries can use different physical jamming devices like EMP weapons or electronic jamming equipment to sabotage the digital and electrical systems of MASS to achieve their objectives. For example, pirates may secrete jammers into containers onboard the MASS to jam the vessel positioning system and stop the vessel at sea in order to steal cargoes by ship-to-ship transfer of cargoes.
Cyber vulnerabilities of SCC and port systems	For shoreside, the port facilities and SCC require high exposure to the internet and the exchange of satellite and radio signals. Different adversaries can use different physical jamming devices to sabotage the electrical and digital systems of the SCC and port systems. For example, terrorists use jammers to sabotage targeted port's traffic systems to cause chaos and slow down port activities of the nation's supply chain, damaging the state's economies.

Table 13. Analysis of the security threat of hybrid security in MASS operations

4. Findings

This paper uses a threat matrix to analyse the risk of the six identified security threats on DOA 4 MASS operations based on the above discussion, the explanation on threat matrix and assessment results are shown in table form below:

	Rare	Moderate	Very Likely
Low Impact	Low Risk	Low Risk	Medium Risk
Medium Impact	Low Risk	Medium Risk	High Risk
High Impact	Medium Risk	High Risk	High Risk

Table 14. Explanation of threat matrix

Very Likely	1. Threats that could occur in various locations. 2. Threats that could be performed by various methods. 3. Most adversaries are highly motivated. 4. Most adversaries have adequate resources to perform the attacks. 5. The attacks on DOA 4 MASS operations are more likely than conventional shipping operations. 6. The attacks on DOA 4 MASS operations are more effective than conventional shipping operations. 7. The security loopholes can be frequently exploited by adversaries if countermeasures of the targets cannot effectively counter the threats.
Moderate	1. Threats that could occur in several locations. 2. Threats that could be performed by several methods. 3. A certain number of adversaries are highly motivated. 4. A certain number of adversaries have adequate resources to perform the attacks. 5. The likelihood of the attacks on DOA 4 MASS operations is similar to that of conventional shipping operations. 6. The effectiveness of the attacks on DOA 4 MASS operations is similar to that of conventional shipping operations. 7. The security loopholes can be exploited by adversaries if countermeasures of the targets cannot effectively counter the threats.
Rare	1. Threats that could only occur in limited locations. 2. Threats that could only be performed by limited methods. 3. Few adversaries are highly motivated. 4. Few adversaries have adequate resources to perform the attacks. 5. The attacks on DOA 4 MASS operations are less likely than conventional shipping operations, or the attacks on conventional shipping operations are already rare. 6. The attacks on DOA 4 MASS operations are less effective than conventional shipping operations.

Table 15. Explanation of likelihood criteria

High	1. Threats that can cause a significant number of casualties. 2. Threats that can cause serious damage to multiple properties. 3. Threats that can cause large scale environmental pollution. 4. Threats that bring significant financial loss to various victims. 5. Threats that bring significant reputational damage to various victims. 6. The impact of the attacks on DOA 4 MASS operations is higher than that of conventional shipping operations.
Medium	1. Threats that can cause a certain degree of casualties. 2. Threats that can cause a certain degree of damage to properties. 3. Threats that can cause a certain degree of environmental pollution. 4. Threats that bring a certain degree of financial loss to victims. 5. Threats that bring a certain degree of reputational damage to victims. 6. The impact of the attacks on DOA 4 MASS operations is similar to that of conventional shipping

	operations.
Low	1. Threats that cause a minor effect to human life, properties, environment, economies, and reputation of the victims. 2. The impact of the attacks on DOA 4 MASS operations is lower than that of conventional shipping operations, or the impact of the attacks is already low in conventional shipping operations.

Table 16. Explanation of impact criteria

Security Threats	Threat Level	Description
Piracy & Armed Robbery at Sea	Likelihood: Moderate Impact: Medium Risk: Medium	**Likelihood**: Conventional physical attacks are less likely due to the reduced effectiveness and return of attacking an unmanned vessel. However, cyber-attacks become more likely due to the cyber characteristics of DOA 4 MASS and the funding from terrorists and organised crime groups. The attacks are mainly carried out when the MASS are sailing at sea, either by approaching the vessel or in distance. **Impact**: Piracy activities can bring significant financial loss to the shipping companies as DOA 4 MASS may be more expensive to be built than conventional manned vessels. Reputation damage can be brought to the shipping companies too. However, piracy activities on DOA 4 MASS operations may not cause significant casualties and damage to the properties and environment, as the major objective of the piracy activities is to extort money.
Terrorism	Likelihood: Very likely Impact: High Risk: High	**Likelihood**: Terrorists have strong motivation to attack shipping industries. Terrorists with sufficient resources can carry out various kinds of attacks including cyber and hybrid attacks on DOA 4 MASS operations which may have more cyber vulnerabilities compared with conventional shipping operations due to its integrated cyber characteristics. The attacks can be carried out in various locations not limited to at sea, either by onsite terrorists or at distance. **Impact**: Terrorism activities on DOA 4 MASS operations can cause serious casualties and environmental and properties damage. The attack can also bring significant financial loss and reputation damage to the companies, ports, and government.
Smuggling and Trafficking	Likelihood: Very likely Impact: Medium Risk: High	**Likelihood**: Smuggling and trafficking issues are common in shipping industries, especially in port activities. They are even more effective and likely to occur in DOA 4 MASS operations if the security of ports and ships are inadequate due to the reduced number of personnel during the operations, especially for the detection/monitoring equipment and the cyber security aspects. The criminal activities involve organised crime groups that have adequate resources. **Impact:** Smuggling and Trafficking can bring significant financial loss, crimes, legal and social issues to the states, shipping companies and ports. However, it seems that the impact of these activities on DOA 4 MASS operations will not significantly diverge from that of conventional shipping operations.
Stowaways	Likelihood: Moderate Impact: Medium Risk: Medium	**Likelihood**: Stowaways are common in shipping industries, especially in port activities. The issue may also frequently occur in DOA 4 MASS operations if the security of ports and ships are loose

		due to the reduced number of personnel during the operations, especially for the detection/monitoring equipment. However, the characteristics of DOA 4 MASS may not favour the stowaways when she is sailing at sea. **Impact**: Stowaways can cause significant financial loss and reputation damage to the shipping companies and states. However, the impact of these activities on DOA 4 MASS operations is similar to conventional shipping operations.
Cyber security threat	Likelihood: Very likely Impact: High Risk: High	**Likelihood**: Various kinds of cyber-attacks can be carried out by various types of adversaries with different objectives. DOA 4 MASS operations may require internet access, exchange of signals and high exposure to the internet to maintain its function, which may expose more cyber vulnerabilities for the attackers. **Impacts**: Cyber security threats can cause significant damage to the systems of DOA 4 MASS operations. The integration of IT and OT systems could cause significant casualties and damage to properties and the environment. Cyber incidents bring significant financial loss and damage of reputation to the shipping companies, ports, and states.
Hybrid security threat	Likelihood: Very likely Impact: High Risk: High	**Likelihood**: Various kinds of hybrid attacks can be carried out by various types of adversaries with different objectives. The majority of DOA 4 MASS operations may require internet access, exchange of signals and high exposure to the internet to maintain its function, which the hybrid attacks on DOA 4 MASS operations may become more effective than conventional shipping operations as more systems can be damaged by hybrid attacks. **Impacts**: Hybrid security threats can cause significant damage to the systems of DOA 4 MASS operations, which the integration of IT and OT systems can cause significant casualties and damage to properties and the environment. Hybrid attacks incidents bring significant financial loss and damage of reputation to the shipping companies, ports, and states.

Table 17. Threats assessment results

Cyber security: Cyber security of the vessel, SCC and port terminal is crucial for DOA 4 MASS operations as a secure cyber defence of MASS can effectively deny a significant amount of attacking methods from different security threats on DOA 4 MASS. Since cyber-attacks occurred only when MASS systems are accessing the internet or exchanging signals, the usage of burst transmission or data burst in DOA 4 MASS operations may reduce the number of exchanging satellite signals and access to the internet, hence reducing the chance of suffering a cyber-attack due to the reduced window of attacking. This paper also finds that the suggestions from The Guideline on Cyber Security Onboard Ships V4 (2020) and the application of current guidelines and requirements of cyber security for the shipping industries such as ISM Code may still be effective for the cyber security of SCC and port terminals in DOA 4 MASS operations. This paper believes the application of these guidelines may be able to support the future instruments regarding DOA 4 MASS operations. For example, shipping companies are required to develop a Safety Management System (SMS) approved by the authority for the SCC to operate DOA 4 MASS according to the new instruments, the company should also train staff to be aware of cyber threats, which the personnel can detect suspicious activities such as suspicious signal loss of MASS and report potential cyber incidents.

Detection/monitoring equipment: Detection/monitoring equipment is important for the physical security of DOA 4 MASS operations at sea and in port. This equipment allows the monitoring of the situation and increases the chance of detecting any security threats that rely on evading detection such as unauthorised person boarding the ship or entering ship/port interface to smuggle goods, then further actions can be carried out to respond to the threats. For criminal activities in ports, the lack of port staff to check the content inside the containers may also pose potential security threats to DOA 4 MASS operations. This paper finds that the requirement of IMO The Guidelines regarding the Verified Gross Mass of a Container Carrying Cargo (2014) which the shipper should provide the verified weight of the containers in the shipping document according to the guideline and submit it to the corresponding representative may further be supported by the usage of advanced equipment to weigh or scan the containers by port and SCC representative in order to enhance the cargoes security.

Reliability of vessel systems: Reliability of the DOA 4 MASS systems directly affect the safety and security of the vessel operations. For example, the reliability of the BAS sensors can affect whether the MASS are able to detect nearby objects, hence avoiding accidents like collision or detecting abnormal situations such as multiple suspicious boats or unknown divers are approaching, which may be scenarios of physical attacks by pirates or traffickers.

Security in SCC: Physical security of SCC may also affect the security of DOA 4 MASS operations. For example, locating SCC in a secure place, hiring security guards, checking, and recording the identity of the personnel entering and leaving the facilities, using scanning equipment to check the personnel belonging, etc. These measures can prevent potential security breaches and unauthorised persons entering SCC to carry out criminal activities like terrorists using firearms to storm SCC and remote control the MASS fleet. Also, the competence of SCC personnel allows them to gain access to the monitoring and controlling of DOA 4 MASS operations, which the criminals may target the SCC personnel vulnerabilities or bribe them to assist their criminal activities during DOA 4 MASS operations.

Security in ports: Several international regulatory frameworks and instruments may still be effective for security in ports. For example, some regulations from ISPS Code (2003) that regulate terrorism and stowaways can be adjusted and applied to DOA 4 MASS operations, such as keeping the application of the security level, security plan and ship security alert systems while using detection equipment like passive infrared sensors and CCTV instead of humans to detect any suspicious terrorist activities in port and onboard. Another example is the IMO MSC Revised guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic (2006) which several measures can still be applied to DOA 4 MASS, such as the personnel access to ship/port interface may be totally restricted as the operations can be carried out without onsite staff, hence, no one should be allowed to enter the area in normal circumstances.

5. Conclusion

The Characteristics of DOA 4 (Degree of Autonomy 4) MASS (Maritime Autonomous Surface Ships') operations may still pose vulnerabilities that can be exploited by all the identified security threats.

For piracy and armed robbery at sea, although the conventional physical attacks by pirates such as boarding the vessel to hijack the ship would be less likely and effective on DOA 4 MASS, successful cyber and hybrid attacks by pirates can allow them to achieve various goals such as stealing cargoes without being detected and hijacking vessel for ransom.

For terrorism, terrorists may secrete explosives onboard MASS if the detectability of the ship, SCC and port are not effective, successful cyber and hybrid attacks on MASS operations can allow them to achieve various goals such as hijacking vessels for terrorist's attacks and disrupting port activities.

For smuggling and trafficking, the criminals may secrete goods onboard MASS if the detectability of the ship, SCC and port are not effective, successful cyber and hybrid attacks by criminals can allow them effectively to smuggle and traffic their goods without being detected.

Stowaways may use a more conventional method to secrete aboard, this can be achieved if the detectability of the ship, SCC and port are not effective. When stowaways secrete onboard and the ship is sailing at sea, the issue becomes more complex, the best way to prevent stowaways' is to prevent them stowing away in port.

For cyber and hybrid security threats, the systems of DOA 4 MASS, SCC and port facilities can be vulnerable to various cyber and hybrid attacks carried out by different attackers with different objectives.

The findings of this paper observe that the risk of terrorism, smuggling & trafficking, cyber security, and hybrid security threats are high in DOA 4 MASS operations, while the risk of piracy and armed robbery at sea and stowaways are medium.

Both the aspects of cyber security, detection/monitoring equipment, reliability of vessel systems, security in SCC and security in ports contribute significantly to the security of DOA 4 MASS operations against these security threats.

6. Recommendations

6.1 Development of future instruments for MASS

All the aspects mentioned in the findings section: cyber security, detection/monitoring equipment, reliability of vessel systems, security in SCC and security in ports should be included, well defined, explained, even making it mandatory and enforced in the future instruments for the stakeholders involved in DOA 4 MASS operations such as flag states, ship classification societies, port state controls and shipping companies, etc. in order to ensure the security of DOA 4 MASS operations against these threats. Disparity and definition gaps between the current instruments and the crimes committed against DOA 4 MASS should be well defined in future instruments.

6.2 Application of cyber security measures

Due to the high likelihood and impact of the potential cyber and hybrid attacks from different security threats on DOA 4 MASS operations, both the stakeholders of shipping companies and port operators should take any possible measure to secure the cyber defence of all systems related to DOA 4 MASS operations, even beyond the legal requirement of the future instruments. The development of the measures may refer to The Guideline on Cyber Security Onboard Ships V4, (2020) at this stage.

6.3 Application of detection/monitoring equipment

Both the stakeholders of shipping companies and port operators should apply any possible equipment in order to increase the chance of detecting security threats, even beyond the legal requirement of the future instruments. Basic detection/monitoring equipment such as CCTV is suggested to be installed on all autonomous vessels which can fully cover the hidden space of the ship, and in port which can fully cover the ship/port interface. While advanced detection/monitoring equipment such as drones and passive infra-red sensors are encouraged to be installed too.

6.4 SCC security and personnel management

Due to the competence of SCC systems and personnel allowing them to gain access to the monitoring and controlling of DOA 4 MASS operations, the responsible personnel should be carefully selected, and the company may develop a confidential reporting system that the staff can trust (Smith, 2020). Physical security measures of SCC such as secure location and hiring security guards are also recommended to be applied as much as possible.

6.5 Carrying out further research

Further research on the identified security threats on DOA 4 MASS operations is recommended to further enhance the analysis and recommendations once more practical data on DOA 4 MASS operations are available. The research on different DOA of MASS operations and different security threats are also recommended to further enhance the security of all DOA MASS operations.

8. References

Bateman, T. (2013, Oct 16). Police warning after drug traffickers' cyber-attacks. *BBC News*.
https://www.bbc.co.uk/news/world-europe-24539417

Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean, and Arabian Sea. (2018). *Version 5*.

Dryad Global. (2021). *Stowaways*.
https://dg.dryadglobal.com/stowaways

Elegant, S. (2004, Aug 23). The Return of Abu Sayyaf. *Time.*
https://web.archive.org/web/20071111084619/http://www.time.com/time/magazine/article/0,9171,686107,00.html

Foster, P. (2013, Apr 23). "Bogus" AP tweet about explosion at the White House wipes billions off US markets. *The Telegraph.*
http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

Gardner, F. (2020, Oct 26). Tanker Stowaways: Seven Men Arrested Over Ship's 'Hijacking'. *BBC News.*
https://www.bbc.co.uk/news/uk-england-hampshire-54687379

Goward, D. (2017, Jul 11). MASS GPS Spoofing Attack in Black Sea. *The Maritime Executive*.
https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

International Maritime Organisation. (2006). Revised guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic. *RES MSC. 228(82).*

International Maritime Organisation. (2014). The Guidelines regarding the Verified Gross Mass of a Container Carrying Cargo. *MSC. 1/Circ. 1475.*

International Maritime Organisation. (2021). Outcome of the Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships. *MSC.1/Circ. 1638*.

International Ships and Port Facility Security Code. (2003).

Jalonen, R., Tuominen, R. and Wahlström, M. (2017). *Safety of Unmanned Ships: Safe Shipping with Autonomous and Remote-Controlled Ships.* Science + Technology, 5/2017.

Kavallieratos, G., Katsikas, S. and Gkioulos, V. (2019). Cyber-attacks Against the Autonomous Ship. *Computer security,* p.20-36.

Kavallieratos, G., Katsikas, S. and Gkioulos, V. (2020). Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. *Intelligent Information and Database Systems,* p.202-217.

Liput, A. L. (1985). An Analysis of the Achille Lauro Affair: Towards an Effective and Legal Method of Bringing International Terrorists to Justice. *Fordham International Law Journal, 9*(2), 5.

Miller, G. (2021, Apr 5). How shipping giant MSC reacted to billion-dollar cocaine bust. *American Shipper.*
https://www.freightwaves.com/news/how-container-giant-msc-reacted-to-billion-dollar-cocaine-bust

Mirror. (2008, Nov 27). *Mumbai attack: TimeLine of how the terror unfolded*.
https://www.mirror.co.uk/news/uk-news/mumbai-attack-timeline-of-how-the-terror-362565

Mudi, M. (2011, Dec 3). Kenya: Oil Tanker Hijacked by Pirates in April Now Released. *AllAfrica.*
https://allafrica.com/stories/201112030215.html

Novet, J. (2017). Shipping company Maersk says June cyberattack could cost it up to $300 million. *CNBC.* https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

Olimpio, M. (2018, Sep 27). Remote Controlled Terror: Houthi Suicide Boats. *European Eye on Radicalization*.
https://eeradicalization.com/remote controlled-terror-houthi-suicide-boats/

O' Neill, D. (2021, Sep 3). Latest cyber-attacks shut down South African ports. *Marine Professional*.
https://www.imarest.org/themarineprofessional/on-the-radar/6214-latest-cyber attacks-shuts-down-south-african-ports?utm_source=email&utm_medium=TMP%20Weekly&utm_campaign=06-09-2021%20
Pasternack, A. (2013). *To Move Drugs, Traffickers are Hacking Shipping Containers.*
https://www.vice.com/en/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs
Satelles. (2019, Aug 7). *Shipping Industry Faces GPD Disruption in Persian Gulf.*
https://satelles.com/shipping-industry-faces-gps-jamming-in-persian-gulf/
Schneider, P. and Winkler, M. (2013). The Robbin Hood Narrative: A Discussion of Empirical and Ethical Legitimizations of Somali Pirates. *Ocean Development and International Law, 44*(2), p.185.
ShipInsight. (2021, Jun 25). *Successful trial of automated trucks in the Port of Hamburg*.
https://shipinsight.com/articles/successful-trial-of-automated-trucks-in-the-port-of-hamburg/
Smith, M. (2020, May 22). Drug Trafficking on Ships. *North.*
https://www.nepia.com/articles/drug-trafficking-on-ships/
Solum, A., Åsgård, B. L. and Urdahl, K. (2021). Ship operations at increased risk of drug smuggling. *Gard*.
https://www.gard.no/web/updates/content/31640962/ship-operators-at-increased-risk-of-drug-smuggling
Tam, K. and Jones, K. (2018). Cyber-Risk Assessment for Autonomous Ships. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* p.1-8.
The Guideline on Cyber Security Onboard Ships. (2020). *Version 4*.
The Maritime Executive. (2021, June 2). *Drewey: Industry will face increasing shortage of officers by 2026*.
https://www.maritime-executive.com/article/industry-will-face-increasing-shortage-of-officers-by-2026-says-drewry
Ung, S.T. (2019). Evaluation of human error contribution to oil tanker collision using fault tree analysis and modified fuzzy Bayesian Network based CREAM. *Ocean Engineering, 179,* 159-172.
United Nations Conference on Trade and Development. (2020). *Review of Maritime Transport*.
United Nations Office on Drugs and Crime. (2017). *The Drug Problem and Organised Crime, Illicit Financial Flows, Corruption and Terrorism*.
Vinnem, J. E. and Utne, I. B. (2018). Risk from cyberattacks on autonomous ships. *Safety and Reliability - Safe Societies in a Changing World*. Taylor & Francis Group.
Washington State Department of Health. (2003). Electromagnetic Pulse (EMP). *Fact Sheet 320-090*.