J. East Asia & Int'l L. Vol. 16/No.2 (2023); 233-250
Publication type : Research Article
Section : Issue Focus
DOI : http://dx.doi.org/10.14330/jeail.2023.16.2.02

Regulating Cyber Security of Maritime Autonomous Surface Ship: New Challenges and Improvements

Junghwan Choi* & Jiancuo Qi**

The development of autonomous ships relies heavily on the Internet technologies, which have introduced a new type of risk to the shipping industry. Increasing dependence on the Internet computing and satellite communications makes cybersecurity a significant consideration for the current operation and future development of autonomy technology in the shipping industry. Cyber risks will be a more critical issue for maritime autonomous surface ships (MASS). This research identifies current international regulatory issues concerning cybersecurity in MASS, and exam ines potential regulatory improvements for the effective prevention and control of potential cyber risks. In terms of improvements, the authors suggest the adoption of a mandatory goal-based MASS code that constitutes an independent cyber risk management, separate from existing safety management systems based on the International Safety Management code. In addition, the SUA Convention for the suppression of unlawful acts against shipping must be revised to actively respond to cyber-crime as an emerging threat in the era of MASS.

Keywords
MASS, IMO, Cyber Risk, Maritime Cyber Risk Management, International Maritime Safety Management Code

* Associate Professor at Law School of Dalian Maritime University, China. LL.M. (Korea Mar. & Ocean Univ.), LL.M. (Swansea U.), Ph.D. (Exeter). ORCID: https://orcid.org/0000-0001-8527-3371. The author may be contacted at: junghwanchoi@dlmu.edu.cn / Address: Law School, Dalian Maritime University, No.1 Liaoning Road, Dalian, Liaoning 116026, P.R. China.

** Corresponding author. Associate Research Fellow of Institute of Maritime Law at Shanghai Maritime University. B.A. (Dalian Mar. U.), LL.M. (Swansea U.), Ph.D. (Korea U.). ORCID: https://orcid.org/0000-0001-5468-2914. The author may be contacted at: qizixin2009@live.cn /Address: Shanghai Maritime University School of Law, 1550 Haigang Avenue, Pudong District, Shanghai 201306 P.R. China.

All the websites cited in this article were last visited on October 26, 2023.

I. Introduction

Today, technological innovation in the aviation, automobile, and information and communication sectors has caused a wave of grand shift in the shipping and shipbuilding sectors.[1] Voices have grown thus louder recently over the need to introduce autonomous ships equipped with automation, eco-friendliness, digitalization, and artificial intelligence (AI). Autonomous ships can contribute to reducing the operational costs of ships by replacing traditional crews with AI systems; preventing marine accidents caused by human factors; and operating ships reliably and efficiently.

The emergence of autonomous ships in maritime transport seems inevitable. However, if such ships are to be commercialized, complex issues will arise. The impact of new technologies and the challenges that come with them, especially in terms of maritime operations, should be assessed from both a technical and a regulatory perspective. In addition to the technical requirements for autonomous operation on ships, a new generation of naval architects, technicians, and engineers will also be needed at the shore-side. The challenges are not merely technical; accommodating existing legal regimes to new developments is another essential consideration.

In 2018, the International Maritime Organization (IMO) provided the official definition of an autonomous vessel as a "maritime autonomous surface ship" (MASS). It also initiated a regulatory scoping exercise, in order to determine how MASS is implemented or incorporated into existing IMO conventions and instruments, as well as assessing its safety and security.[2] In this regard, some in the international community have expressed concerns about cyber-attacks, since MASS will be developed by AI and advanced computer systems. MASS may be vulnerable to indiscriminate or targeted cyber-attacks if a shipping company or shore-operator does not properly establish cyber risk management protocols or a cybersecurity system.[3] This vulnerability can be attributed to the increase in network connections and

1 Koji Wariishi, *Maritime Autonomous Surface Ships: Development Trends and Prospects-How Digitalization Drives Changes in Maritime Industry*, Mitsui & Co. Glob. Strategic Stud. Inst. Monthly Rep. (2019), https://www.mitsui.com/mgssi/en/report/detail/__icsFiles/afieldfile/2020/01/09/1909t_wariishi_e.pdf; Rolls-Royce, *Autonomous ships: The Next Step*, Mar. Ship Intel. (2017), https://www.rolls-royce.com/~/media/Files/R/Rolls Royce/documents/%20customers/marine/ship-intel/rr-ship-intel-aawa-8pg.pdf.

2 IMO Doc. MSC/99/22, https://iadc.org/wp-content/uploads/2018/07/MSC-99-22-Report-Of-The-Maritime-Safety-Committee-On-Its-Ninety-Ninth-Session-Secretariat.pdf.

3 The Maritime Executive, Cybersecurity Risk Remains the Leading Concern for Autonomous Shipping, https://maritime-executive.com/editorials/cybersecurity-risk-remains-the-leading-concern-for-autonomous-shipping.

information exchange between ships, land-based facilities, and critical ship systems. Specifically, the operation of autonomous ships necessitates advanced remote-control technology. Failure to ensure cybersecurity in remote control communications can result in even significant maritime accidents.

The objective of this research is to underscore the imperative need for a regulatory framework governing cybersecurity in MASS. This is crucial for averting potential cyber threats and incidents. This paper will begin with providing an overview of the current state of MASS technology and the escalating cyber risks within the shipping industry. Furthermore, it will scrutinize the existing international regulatory protocols for cybersecurity, as well as the specific challenges and applications in the context of MASS as an emerging technology. The paper will then propose a robust strategy to bolster cybersecurity effectiveness through the establishment of an independent and advanced maritime cyber risk management framework within the MASS code. Additionally, it will advocate for amendments to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA), in order to ensure an appropriate response to cyber-crimes.[4] Finally, the authors will advocate for the inclusion of coverage for damages resulting from cyber incidents and related risks within insurance policies, thus providing a comprehensive approach to managing cybersecurity in the realm of MASS.

II. General Consideration of MASS and Cyber Risk Issues

A. Introduction of MASS as a New Technology

In recent, countries with interest in providing international shipping services have seen a surge in interest in MASS for freight transportation. Notably, James Fanshawe, chair of the UK's Maritime Autonomous Systems Regulatory Group, has emphasized the imminent necessity of autonomy for the industrial revolution.[5] This shift will rely on technology replicating human influence in ship operations, evolving them through complex autonomous systems that make operational decisions. The development and application of AI technology are intended to liberate manpower from repetitive, programmed tasks and enable individuals to focus more on creative mental work.

4 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation [SUA], https://www.imo.org/en/About/Conventions/Pages/SUA-Treaties.aspx.

5 Varsha Saraogi, *How will Autonomy Shape the UK Shipping Industry?*, Ship Tech. (July 30, 2022), https://www.ship-technology.com/analysis/how-will-autonomy-shape-the-uk-shipping-industry.

The need for safe vehicular transportation systems in general is paramount and vital, given that reported deaths due to traffic accidents exceed 1.35 million worldwide, with 94 percent attributed to human error, such as fatigue and distracted driving.[6]

Shipping, one of humanity's oldest industries, faces significant challenges brought about by AI, the most representative revolution of which is the emergence of autonomous ships. Interest in autonomous vehicles has been growing in the industry for some time and, in recent years, the concept of 'autonomy' and MASS have attracted attention across the maritime sector. AI, which simulates human intelligence by harnessing computer technology, has been applied in the maritime field since the 1970s for remotely operating underwater vehicles for research and military purposes.[7] Advances are announced frequently by established and new tech players alike. In 2012, for instance, the unmanned vehicle PAPA MAU demonstrated the potential of unmanned long-distance sailing, crossing the Pacific from San Francisco to Bundaberg.[8] The European Union (EU), China, Japan, and South Korea have made notable strides in developing autonomous ships, such as the EU's investment in the MUNIN project[9] and China's autonomous ship test site in Zhuhai.[10] Furthermore, Japan's MEGURI2040 project conducted extensive autonomous ship tests,[11] while South Korea achieved the world's first autonomous transoceanic voyage of a large LNG carrier.[12] Although these developments are largely in the experimental phase, autonomous ships are set to become the primary tools of future shipping. Projected to reach a market size of USD 14.2 billion by 2030, the benefits of autonomous ships, both economically and environmentally, would serve as the driving force of their own development.[13]

With regard to general descriptions and definitions of MASS, the IMO is assessing the existing framework to examine how to apply it according to different degrees of

6 Ahmed Jubaer et al., *How does Emotional Intelligence Predict Driving Behaviours among Non-Commercial Drivers?*, 85 Transp. Res. F: Traffic Psychol. 38 (2022).

7 Daniel Vallejo, *Electric Currents: Programming Legal Status into Autonomous Unmanned Maritime Vehicles*, 47(1) Case W. Res. J. Int'l L. 413 (2015).

8 Paul Pritchett, *Ghost Ships: Why the Law Should Embrace Unmanned Vessel Technology,* 40 Tul. Mar. L. J. 197 (2015).

9 Maritime Unmanned Navigation through Intelligence in Networks [MUNIN], http://www.unmanned-ship.org/munin.

10 Safety4Sea, China Builds Asia's First Autonomous Ship Test Area, https://safety4sea.com/china-builds-asias-first-autonomous-ship-test-area.

11 The Nippon Foundation, The Nippon Foundation MEGURI2040 Fully Autonomous Ship Program, https://www.nippon-foundation.or.jp/en/news/Art.s/2022/20220118-66716.html.

12 Safety4Sea, World's First Transoceanic Trip of LNG Carrier Using Autonomous Navigation Takes Place, https://safety4sea.com/worlds-first-transoceanic-trip-of-lng-carrier-using-autonomous-navigation-takes-place.

13 *NA Proactive news snapshot,* Proactive News, (June 15, 2022), https://www.proactiveinvestors.com/companies/news/984919/na-proactive-news-snapshot-chesapeake-financial-shares-dore-copper-mining-sidus-space-neo-battery-materials-valeo-pharma-looking-glass-labs-update-984919.html.

automation. At the 99th Maritime Safety Committee (MSC) meeting, held in May 2018, the IMO for the first time provided a definition of different degrees of autonomy for ships, classifying them according to four levels:[14]

Table 1: Autonomy Level of MASS [15]

Degree Level	Description of the Autonomous Level
Degree 1	Ship with automated processes and decision support: Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated.
Degree 2	Remotely controlled ship with seafarers on board: The ship is controlled and operated from another location, but seafarers are on board.
Degree 3	Remotely controlled ship without seafarers on board: The ship is controlled and operated from another location. There are no seafarers on board.
Degree 4	Fully autonomous ship: The operating system of the ship is able to make decisions and determine actions by itself.

B. Benefits of MASS

The MUNIN project in 2016 was one of the most influential research programmes for developing "a technical concept for the operation of autonomous merchant vessels" and assessing its "technical, economic, and legal feasibility."[16] Similar studies have been conducted to identify the technological and legislative factors that might obstruct the development of autonomous shipping. AI, the so-called Internet of Things, and robotics all promise to create new opportunities and benefits for society. Autonomous ships offer significant potential for reshaping and enhancing the efficiency and sustainability of maritime trade. Through the integration of information technology (IT) and AI, they aim to bolster safety, reliability, energy conservation, environmental protection, and operational efficiency. These innovations could also substantially minimize, if not eradicate, maritime collision incidents. The potential benefits of autonomy can be divided into four broad areas:

14 MUNIN, *supra* note 9.

15 Analysis of Regulatory Barriers to the use of Autonomous Ships Submitted by Denmark, IMO Doc. MSC 99/INF.3, https://dma.dk/Media/637745499808186153/Analysis%20of%20Regulatory%20Barriers%20to%20the%20Use%20of%20Autonomous%20Ships.pdf.

16 *Id.*

1. Enhancing maritime safety: Studies suggest that approximately 70% of marine accidents are attributable to human errors or improper navigation.[17] The adoption of advanced automation in shipping could mitigate these occurrences, as autonomous ships leverage automatic sensing technology and intelligent decision-making systems to eliminate human-related mishaps.[18] In high-traffic waterways, technology facilitates monitoring and communication between vessels, thus reducing operational risks. Additionally, emergency response capabilities are enhanced through distress warning and rescue technology, while route-planning technologies can ensure the optimization of safe and economical routes.

2. Economic viability: With the ever-increasing demands of global trade, the implementation of energy efficiency management and control technology on autonomous vessels is projected to improve energy efficiency significantly. This translates to both economic and environmental benefits by reducing fuel consumption and operational costs.[19] The elimination of crew-related expenses such as accommodation and wages also leads to cost reduction, as these vessels require less weight, offer more cargo space, and have decreased fuel requirements. Furthermore, the adoption of condition monitoring and fault diagnosis technology ensures potential risks are mitigated and maintenance costs are minimized.

3. Commitment to environmental sustainability: The maritime industry's impact on the environment, particularly in terms of pollution and greenhouse gas emissions, necessitates a proactive approach to sustainable practices. Autonomy, through digital software, can significantly contribute to reducing emissions by enabling extensive fuel savings.[20] For instance, the autonomous vessel Yara Birkeland, launched in November 2020, is estimated to save up to 90 percent in annual operating costs compared with similar-sized conventional vessels. It would also replace the equivalent of 40,000 truck journeys annually, reducing local pollution and greenhouse gas emissions accordingly.[21]

4. Facilitating industry evolution: Autonomous navigation technology represents a disruptive force in the maritime industry.[22] Its adoption is expected to lead to a decrease in construction and operating costs, due to reduced crew size and

17 Andrea Galieriková, *The Human Factor and Maritime Safety*, 40 Transp. Res. Procedia 1320 (2019).

18 Wróbel Krzysztof, Montewka Jakub & Kujala Pentti, *Towards the Assessment of Potential Impact of Unmanned Vessels on Maritime Transportation Safety*, 165 Reliability Engineering & Sys. Safety 163 (2017).

19 Pritchett, *supra* note 8, at 201.

20 IMO Strategy on Reduction of GHG Emissions from Ships, https://www.imo.org/en/MediaCentre/HotTopics/Pages/Cutting-GHG-emissions.aspx.

21 Business Norway, The World's First Zero-emission Autonomous Container Ship, https://www.theexplorer.no/solutions/yara-birkeland--the-worlds-first-zero-emission-autonomous-container-ship.

22 Vasile-Daniel Păvăloaia & Sabina-Cristiana Necula, *Artificial Intelligence as A Disruptive Technology—A Systematic Literature Review*, 12(5) Electronics 1102 (2023).

subsequent freeing-up of space and resources.

Moreover, as labour costs continue to rise, autonomous vessels can provide economic benefits in a longer term despite their substantial initial investment. With better working conditions onshore, the human factor, a primary source of maritime accidents, is significantly mitigated in autonomous navigation.

In conclusion, given their numerous benefits, autonomous ships can be considered the future of the shipping industry. The emergence of autonomous ship may also alleviate the global shortage of seafarers due to a declining interest in maritime careers, so that it could constitute a long-term trend rather than a fleeting technological innovation.[23]

C. Increased Risk of Maritime Cyber-Attacks

The IMO provides that "maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised."[24] The Baltic and International Maritime Council (BIMCO) provides a further definition of a cyber-attack as "any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and ship systems and data."[25]

The development of autonomous ships relies heavily on the Internet technologies, which have introduced a new type of risk to the shipping industry. Cybersecurity is one of such key challenges and countering cyber-attacks is imperative for shipping companies.[26] MASS depends heavily on computers and other robotic equipment, which could exacerbate vulnerability to such attacks.[27] There are several different vessels that operate in various environments and tend to use different computer systems. Many of these are outdated, running on operating systems that are no longer

23 Aldo Chircop, *Testing International Legal Regimes: e Advent of Automated Commercial Vessels*, 60(1) Ger. Y.B. Int'l L. 4 (2018).

24 Guidelines on Maritime Cyber Risk Management, IMO Doc. MSC-FAL.1/Circ.3/Rev.1.

25 BIMCO, The Guidelines on Cyber Security Onboard Ships, at 58, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

26 Sungbaek Cho et al., *Cybersecurity Considerations in Autonomous Ships*, NATO Cooperative Cyber Defence Centre of Excellence: Tallinn (2022), at 5, https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf.

27 Jonathan Earthy & Margareta Lützhöft, *Autonomous Ships, ICT and Safety Management*, *in* Managing Maritime Safety 146 (Helle Oltedal & Margareta Lützhöft eds., 2018).

supported.[28] The computer systems used at ports and onshore also make maritime operations more vulnerable to cyberattacks.

Damages are no longer limited to owners or operators; they may affect other ships or even entire regions.[29] The inherent vulnerabilities that come with increased use of and reliance upon communication and digital technologies need significant attention. Among the types of cyber-attacks that may impact shipping companies and ships are untargeted attacks, where a company or a ship's systems or data may be just one of several possible targets. By contrast, targeted attacks occur when an organisation, a vessel, its systems or data are the specific focus or one of several planned targets. Such cyber-attacks may result in serious physical damage and loss of property by corrupting the availability of OT and IT systems.

According to Allianz's Safety and Shipping Review 2023, the majority of cyber incidents in the shipping industry thus far have primarily occurred on land.[30] These incidents encompass such activities like ransomware and malware attacks directed at the database systems of shipping companies and ports. As a typical example, in June 2017, A.P. Moeller Maersk, the largest container shipping company globally, fell victim to the 'NotPetya' ransomware cyber-attack. This led to a complete system shutdown that lasted for three weeks, incurring an estimated cost of around USD 300 million.[31]

Attacks have occurred since across the globe. In July 2018, China's government-owned shipping firm, COSCO Shipping, experienced a cyberattack also involving ransomware. This incident affected the Pier Jerminal port operation website and e-mail system in North America, resulting in a three-to-four day period of system failure.[32] In March 2019, certain vessels belonging to HMM, a shipping company based in South Korea, fell victim to a ransomware attack. This resulted in significant harm, as the main on-board computer was rendered inoperable due to being locked by the malware.[33] Operations at the Port of Lisbon were also suspended for four days

28 Keith Martin & Rory Hopcraft, *Why 50,000 Ships are so Vulnerable to Cyberattacks*, Conversation (June 13, 2018), https://theconversation.com/why-50-000-ships-are-so- vulnerable-to-cyberattacks-98041.

29 Darryl Kennard, *Cyber Security and Cyber Risks in the Shipping Industry*, Penningtons Manches Cooper News (July 1, 2019), https://www.penningtonslaw.com/news-publications/latest-news/2019/cyber-security-and-cyber-risks-in-the-shipping-industry.

30 Allianz, Safety and Shipping Review 2023, https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/AGCS-Safety-Shipping-Review-2023.pdf.

31 Craig Allen, *Developing and Implementing a Maritime Cybersecurity Risk Assessment Model,* 31 USF Mar. L. J. 77 (2018).

32 Offshore Energy, COSCO Shipping Lines Falls Victim to Cyber Attack, https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack.

33 Offshore Energy, HMM Hit by Cyber Attack, https://www.offshore-energy.biz/hmm-hit-by-cyber-attack.

after a cyberattack on the port's website and internal computer system on December 25, 2022.[34]

Until now, cyberattacks have been primarily aimed at exploiting security gaps in shipping companies to inflict financial harm. However, the emergence of autonomous ships raises the potential for cyberattacks to escalate to attempts to seize control over the vessel itself. With remote-control capabilities, it becomes plausible to launch simultaneous cyber assaults on multiple ships that share similar specifications and systems, potentially amplifying the scale of damage exponentially. Managing such incidents will pose a considerable challenge.

III. International Regulatory Regime for Cybersecurity and its Implications for MASS

A. Current International Regime for Cybersecurity in the Shipping industry

In 2016, the IMO officially acknowledged the critical importance of cybersecurity, recognizing that security breaches could pose significant threats to the safety and security of ships, ports, and marine facilities.[35] In response, it issued a temporary risk management guideline (MSC.1/Circ.1526), which was later replaced by a formal guideline (MSC-FAL.1/Circ.322).[36] In 2017, the IMO adopted Resolution MSC.428(98), mandating member states to implement a cybersecurity risk management approach within the existing safety management systems of ships.[37]

Cyber risk management encompasses the systematic procedure of recognizing, examining, evaluating, and conveying any risk associated with cyber threats. It involves the decision-making process of either embracing, evading, shifting, or lessening this risk to a level deemed acceptable.[38] The IMO's guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities including functional elements that support effective cyber risk management.[39] As a high-level

34 Safety4Sea, Cyber Attack Hits Port of Lisbon, https://safety4sea.com/cyber-attack-hits-port-of-lisbon.

35 IMO, Maritime Cyber Risk, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

36 *Supra* note 24.

37 IMO Doc. MSC 98/23/Add.1, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

38 *Id.*

39 *Id.*

recommendation, the IMO Resolution MSC.428(98) requires administrations to make certain that cyber risks are adequately incorporated into their current safety management systems, as outlined in the International Safety Management (ISM) Code, by the initial annual verification of the company's Document of Compliance from January 1, 2021.[40]

In Europe, the NIS2 directive (EU Directive 2016/1148) emphasizes the critical importance of cybersecurity within the maritime sector.[41] This directive classifies maritime operators, which encompass passenger and freight water transport companies, as well as the governing bodies of ports and operators of vessel traffic services, as "operators of essential services" (OES).[42] They are strongly advised to enhance their cybersecurity measures. The European Union Agency for Cybersecurity (ENISA) has also been actively involved in bolstering maritime security.[43] Its efforts include the publication of several cybersecurity reports and guidelines tailored for the maritime industry. Notably, back in 2011, they released an inaugural EU report on cybersecurity challenges within the maritime sector.[44] This was followed by a subsequent report in 2019, which focused on security measures for port authorities and terminal operators. The latter report furnished a comprehensive list of potential threats and corresponding security recommendations.[45] Furthermore, in 2020, a more extensive set of risk management guidelines for port security was issued.[46]

In terms of risk management of shipboard systems, BIMCO, in collaboration with other prominent shipping organizations, has also published thorough security guidelines. In July 2019, it adopted an additional cybersecurity clause to be incorporated in maritime contracts.[47] This clause provides for responsibilities between the contracted parties in the event of a cybersecurity incident. In particular,

40 *Id.*

41 Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016. Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&rid=2.

42 *Id.*

43 Cornelia Riehle, EDPS Provides Opinion on Cybersecurity Directive, EUCRIM News (May 20, 2021), https://eucrim.eu/news/edps-provides-opinion-on-cybersecurity-directive.

44 European Network and Information Security Agency, Analysis of Cyber Security Aspects in the Maritime Sector, https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1.

45 European Network and Information Security Agency, Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

46 European Network and Information Security Agency, Guidelines - Cyber Risk Management for Ports, https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.

47 BIMCO, Cyber Security Clause 2019, https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019.

it requires each party to implement appropriate cybersecurity measures and systems, and to ensure appropriate procedures to be in place to allow an efficient and effective response to a cybersecurity incident. In the event of an cyberattack, parties must promptly inform one another and provide additional details within a 12-hour's period.[48] They are also tasked with taking reasonable measures to mitigate and/or resolve the event, while sharing pertinent information to be accessible. However, as BIMCO's Cyber Security Clause 2019 does not address issues related to payment fraud, it lacks any force majeure provisions.[49]

With respect to marine insurance, a majority of marine hull insurance contracts contain a cyber-attack exclusion clause. Typically, the Institute Cyber Attack Exclusion Clause (CL380) excludes coverage if a cybersecurity incident serves as the trigger for a loss that insurers might otherwise be willing to cover.[50] For example, this would include a scenario where a vessel's navigation system is hacked, leading to a grounding and subsequent cargo damage. It is worth noting that the clause applies only to situations involving a cyber-attack. It does not address accidental losses, such as mishaps resulting from a maintenance upgrade gone awry.[51]

B. Regulatory Issues Concerning Cybersecurity of MASS

First of all, the existing legal framework governing maritime transportation is predominantly human-centric, placing significant emphasis on human control as the primary factor for ensuring safety at sea. The United Nations Convention on the Law of the Sea (UNCLOS) regulates, in greater or lesser detail, almost every possible activity on, in, under, and over the sea.[52]

The emergence of MASS will bring change of manning requirements and new

48 *Id.*

49 *Id.*

50 Institute Cyber Attack Exclusion Clause, cl. 380, https://www.allianz.com.tr/content/dam/onemarketing/aztr/allianz/pdf/diger/Tekne-Kloz-Metinleri-04022020.pdf. It states:

1.1 Subject only to Clause 1.2 below, in no case shall this agreement cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system.

1.2 Where this Clause is endorsed on contracts covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software programme, or any electronic system in the launch and/o guidance system and/or firing mechanism of any weapon or missile.

51 *Id.*

52 The overarching goal of the UNCLOS, according to its preamble, is to establish "a legal order for the seas and oceans which will facilitate international communication and will promote the peaceful uses of the seas and oceans, …" For details, *see* James Harrison, Making the Law of the Sea 37 (2011).

challenge to seafarer's competence and qualification.[53] International maritime conventions do not specifically define whether a ship's master should be physically onboard; this is generally determined by the domestic law of each state.[54] Different countries have their own interpretations, leading to significant variations in how the manning of an autonomous vessel is identified. According to Article 94 of the UNCLOS, the flag state exercises jurisdiction over master and crew to ensure maritime safety.[55] Measures should be taken in conjunction with relevant international documents on "the manning of the ship, the working conditions, and training of the crew."[56] These measures ensure that each vessel is under the responsibility of a master and crew who practice good seamanship. However, it is necessary to emphasize that the provision also requires conformity to "generally accepted international regulations, procedures, and practices and to take any steps necessary to secure their observation."[57] In other words, the UNCLOS confers prescriptive rights to flag states by referring to an abstract and continually changing provision. Therefore, it is submitted that the IMO obtains the right to regulate MASS, as the UNCLOS does not 'freeze' the scope of the rules that flag states should observe. In this context, the wording of the UNCLOS should not be construed as a legal barrier to the introduction of autonomous ships to the shipping industry.

Along with jurisdictional and interpretational issues under the UNCLOS, cybersecurity will pose significant challenges with the introduction of MASS. The international shipping industry does not have proper or effective international regulations regarding cybersecurity in MASS.[58] With the advent of either a reduced crew or fully unmanned autonomous ships, a surge in "cyber piracy" incidents targeting vessels and their cargo is anticipated. This entails manipulating ships through cyber-attacks to redirect them to specific locations, allowing for the hijacking of both ships and their cargo.

Given the vulnerability of current security measures, successful cyberattacks targeting ports and shipping companies are also poised to escalate. This is largely due to the substantial economic gains and far-reaching repercussions associated with such actions. The prevailing challenge lies in the fact that, while the IMO has urged member states to assess and mitigate the risk of maritime cyber-attacks by

53 Junghwan Choi & Sangil Lee, *Legal Status of the Remote Operator in Maritime Autonomous Surface Ships (MASS) under Maritime Law*, 52(4) Ocean Dev. & Int'l L. 446 (2022).

54 *Id.*

55 UNCLOS art. 94(5).

56 *Id.*

57 *Id.*

58 *Id.*

integrating a cyber safety management system into the existing ISM Code, via the adoption of IMO Resolution MSC.428(98).[59] These guidelines do not carry legally binding status, but stand as a high-level recommendation. In addition, while regional shipping alliances such as BIMCO are taking steps to develop their own response protocols, there remains a notable absence of comprehensive global-level response to phenomena like cyber piracy.

IV. Recommended Improvements to International Regulations for the Mitigation and Control of Cyber Risk in MASS

A. Need for Adoption of Mandatory Resolution or Code for the Safety of MASS

The IMO first proposed the need for regulatory analysis of MASS at the 99th Session of the MSC.[60] In April 2022, the 105th session of the committee produced a roadmap, including a schedule for developing the IMO instruments for MASS.[61] This roadmap envisages the progress of a goal-based instrument in the form of a non-compulsory code, which is expected to be adopted in the second half of 2024 as the first stage.[62] It includes a review of the main principles, purpose, and objectives, scope, and structure of autonomous vessel instrument development, a common understanding of autonomous vessel terminology, and further examines how to address common challenges identified in the IMO instruments, among other things.[63]

The 106th MSC session in November 2022 made further progress on the development of a goal-based instrument regulating the operation of autonomous vessels.[64] It aims to adopt a non-mandatory MASS code, to take effect in 2025. This

59 Klemens Katterbauer, *Shipping of the Future-Cybersecurity Aspects for Autonomous AI-Driven Ships*, 36(1) AUSTL. & N.Z. MAR. L. J. 1 (2022).

60 IMO, Maritime Safety Committee (MSC) 99th Session 16-25 May 2018, https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-99th-session.aspx.

61 Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS), IMO Doc. MSC.1/Circ.1638, https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/MSC.1-Circ.1638%20-%20Outcome%20Of%20The%20Regulatory%20Scoping%20ExerciseFor%20The%20Use%20Of%20Maritime%20Autonomous%20Surface%20Ships...%20(Secretariat).pdf.

62 *Id.*

63 *Id.*

64 IMO, Maritime Safety Committee (MSC 106: Nov. 2-11, 2022), https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-106.aspx.

will form the basis for a mandatory code, scheduled to enter into force on January 1, 2028.[65] The mandatory element of the new MASS code must be ensured through its incorporation as a new chapter in the International Convention for the Safety of Life at Sea (SOLAS).[66]

B. Need for Revision of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation

It is essential that the international community recognizes the gravity of cybersecurity issues in maritime operations and swiftly collaborates on comprehensive countermeasures. In particular, cyber-crime should be clarified as an unlawful act under the SUA. This Convention was devised to overcome the limitations of legislation on acts of piracy, as defined by clauses in the UNCLOS. It extended this remit to unlawful acts committed on or by ships if a vessel "is navigating or is scheduled to navigate into, through, or from waters beyond the outer limit of the territorial sea of a single state, or the lateral limits of its territorial sea with adjacent states," as well as offenses committed within a state's territory.[67]

Unlawful acts for both political and private ends are covered by the SUA. Under the Convention, these include the seizure of vessels by force, acts of violence against persons on board, and the placing of devices on board a ship that are likely to destroy or damage it.[68] The primary objective of the SUA is to guarantee that appropriate measures are taken against individuals who commit unlawful acts against ships.[69] The SUA does not impose territorial constraints. It means that even though the location of the intrusion and the computer system used for this purpose are not within the jurisdiction of the state party, provided the autonomous ship affected is within the state party's territorial waters as a result of the unlawful action, the SUA can still be applied.

The definition of piracy must be updated to reflect advances in autonomous shipping technology. As AI becomes more prevalent in the maritime industry, piracy is likely to merge with cybercrime, resulting in a new category of crime at sea. In addition to traditional acts of piracy, the Internet intrusions should be considered

65 *Id.*

66 International Convention for the Safety of Life at Sea 1974, https://treaties.un.org/doc/Publication/UNTS/Volume%201226/volume-1226-I-18961-English.pdf.

67 SUA art. 6.

68 Brendan Sullivan, *A Tale of Two Treaties: A Maritime Model to Stop the Scourge of Cybercrime*, 39 BU Int'l L. J. 143 (2021).

69 SUA art. 5.

within the scope of piracy, and efforts to ensure the safety of autonomous ships from such remote attacks must be intensified. In developing the MASS code, the IMO needs to revise the SUA to more effectively classify and counteract remote cyber-attacks on autonomous shipping.

C. Increasing the Effectiveness of Maritime Cyber Risk Management Systems

Maritime cyber risk management has been described as "the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders."[70] As stated earlier, the IMO encourages member states to establish maritime cyber risk management systems within the existing ISM Code. Resolution MSC.428(98) requires member states to introduce a risk-based approach when establishing a cyber risk management system, in order to implement it in the most effective manner.[71] However, policy and regulatory discussions about specific maritime cyber risk management systems have been limited so far at the IMO's meetings. Resolution MSC.428(98) exists only as a high-level recommendation, not a mandate.

There are several steps the IMO can take to improve matters. First, a more comprehensive form of independent, international maritime cyber risk management is necessary. Currently, the ISM Code requires ship owners to obtain a Document of Compliance (DoC) and Safety Management Certificate (SMC), issued by the maritime administration of the flag state.[72] A port state can inspect foreign vessels, when the vessel has entered their port, to assess whether she is complying with the ISM Code.[73] This Code stipulates clear provisions for compliance and verification, which set out the legal grounds for port state control. The IMO may consider developing additional provisions for independent maritime cyber risk management as part of its MASS code, to be incorporated in existing practices.[74]

Second, the IMO must make the MASS code mandatory. Given that MASS will be

70 *Supra* note 37.

71 *Id.*

72 Adoption of Amendments to the International Safety Management (ISM) Code, IMO Resolution MSC.104(73), https://wwwcdn.imo.org/localresources/en/OurWork/HumanElement/Documents/104(73).pdf.

73 Procedures for Port State Control 2021, Appendix 8 - Guidelines for Port State Control Officers on the ISM Code, IMO Resolution A.1155(32), https://www.imorules.com/GUID-3758C0AF-E821-465D-BC8C-35264A2A1757.html.

74 Industrial Cyber, Maritime industry needs to adopt appropriate steps for cyber risk management of systems, infrastructure (2023), https://industrialcyber.co/features/maritime-industry-needs-to-adopt-appropriate-steps-for-cyber-risk-management-of-systems-infrastructure.

commercialized soon, there is a need for an explicit international regulatory regime applicable to MASS that takes the management of maritime cyber risk as well as cybersecurity matters in general into account. Verification and compliance regulations should be included while developing the MASS code, to increase its effectiveness. As outlined above in respect to the ISM Code, these provisions would enable both flag state and port state to verify that the vessel is complying with the mandatory provisions of the MASS code.[75]

Lastly, the IMO should either revise Resolution A. 1155(32) - Procedure for Port State Control - , or adopt a new resolution for port state control specific to MASS, considering that the current resolution pertains to conventional ships.[76] New port state control procedures will be needed to enable port state control officers to inspect autonomous vessels effectively. These procedures may comprise inspection methods for maritime cyber risk management, cybersecurity certificates, and documents of compliance that are specific to MASS. Port state control can be an effective way to verify cyber risk management systems between ship and shore and ensure cybersecurity awareness among seafarers.[77]

D. Need for Coverage of Cyber Incidents in Marine Insurance

In general, insurance coverage of damage arising from cyber-attacks is provided for on an ad hoc basis by individual insurance companies. There are still non-binding documents or clauses for the exclusion of cyber incidents in many insurance contracts. For example, the Institute Cyber Attack Exclusion Clause is widely used for malevolent cyber incidents.[78] BIMCO recommends that the insurance market for MASS explicitly insure all risk policies or provides "silent cover," which means all risks may be covered in the contract, including cyber risks, without being mentioned explicitly.[79] In addition, BIMCO has suggested the introduction of "buy back" solutions. This term refers to the option of reinstating a previously excluded risk in the contract, subject to defined conditions and an agreed-upon supplementary premium.[80] This allows for the inclusion of additional cyber coverage.

With the anticipated rise in cyber incidents due to the growing commercialization

75 Gunn Kim & Sang-Il Lee, *A Study on Adaptation of the ISM Code to Maritime Autonomous Surface Ships (MASS),* 34(2) Rev. Mar. L. [해사법연구] 359-96 (2022).

76 *Id.*

77 Aristotelis Komianos, *The autonomous shipping era. operational, regulatory, and quality challenges*, 12(2) Int'l J. Marine Navigation & Safety of Sea Transportation 335-48 (2018).

78 BIMCO, *supra* note 47, at 46.

79 *Id.*

80 *Id.*

of MASS, it is essential to have safeguards in place within insurance contracts to address these risks. This will be essential for encouraging ship owners to operate the MASS vessels. In the coming years, shipping companies will need to engage in a confirmation process with insurers to ascertain whether their policies will provide coverage for physical damage or loss resulting from cyber incidents.

V. Conclusion

To what extent autonomous technology should be integrated into future ships remains an open question for the maritime industry. However, there is no doubt that the development of autonomy will bring a revolution to the shipping market, making autonomous shipping a reality in the future. As a result, the maritime legal regime requires regulatory adjustments to accommodate this development. The challenge lies in determining how best to tackle these emerging issues. Their complexity is due in part to the numerous rules and regulations included in several international instruments over the past few decades, which have been the result of years of negotiations by the international community. Consequently, achieving consensus among member states is critical for reaching an agreement to regulate new autonomy technologies. This is particularly true for some jurisdictions where the revision and approval of legal instruments rely heavily on the decisions of relevant authorities and governments. In addition to legal reform to accommodate technological advancements, the challenge extends to determining the extent to which various parties, such as shipowners, manufacturers, and end users, should be interested in investing in and facing liabilities and insurance issues.

Moreover, countermeasures against cyber risk and the prevention of cyber incidents in MASS will be critical issues in the shipping industry. While the IMO Resolution MSC.428(98) provides cyber risk management to ship owners within the existing ISM Code, it remains a high-level recommendation without binding force. Although MASS will be commercialized soon, there remains a regulatory gap regarding cybersecurity.

Based on this study, the authors will make a few recommendations in a regulatory direction to effectively prevent cyber incidents or cyber-attacks against MASS. First, the IMO needs to develop a goal-based MASS code by including independent maritime cyber risk management procedures. This will be conducive to ensuring that safe measures are adopted in response to cyber incidents and interaction between

ship and shore plays a significant role. The IMO must make the new MASS code mandatory, through its incorporation into the SOLAS as a new chapter. In addition, given that the existing SUA does not contain explicit provisions for "cyber attacks" or "cyber-crime," it needs to be revised to proactively respond to cybercrime and remote attacks such as cyber terrorism. Apart from these IMO regulatory instruments, insurance policies for coverage of damage arising from cyber risks or cyber incident are another prerequisite for the commercialization of MASS.

It should be noted that cyber risks transcend borders and pose inherent challenges in pinpointing culprits. This may shift the liability framework for handling cyber risks in MASS. The insurance sector will have to create innovative marine insurance offerings tailored to these risks and elucidate the responsibilities of contractual parties for smoother handling during the claims process. The international community should recognize that it is of the utmost importance to come up with mandatory legal instruments regarding cybersecurity that deal with interface technology, as well as regulations to safely operate MASS in the future.

Received: August 1, 2023
Modified: September 15, 2023
Accepted: November 1, 2023