Emerging Cyber Technologies in the Maritime Domain: Challenges for Maritime Security and 'Order at Sea'

*Maliha Zeba Khan**
*Muhammad Faisal Sadiq***

ABSTRACT

The global shipping and other commercial and economic activities are backbone for states' political activities, sustainable socioeconomic development, and security. However, traditional concepts of security, order, state, power, warfare, and threat perception besides several others are in transition bringing drastic changes to the contemporary world. Technological advancements, considerable amount of research and development, and evolution of knowledge about different domains have affected all spheres of life, and besides opportunities, number of challenges too have emerged. Maritime realm is the one going through these changes quite vehemently, but this spatial dimension has gathered lesser focus in terms of academic activities, research and establishment of discourse related to its issues. Nevertheless, nature of threats in this domain is more non-traditional than traditional. These non-traditional challenges are also getting transformed and getting complex due to advancement of technology. Particularly, innovation in cyber technology has brought afore a plethora of opportunities in maritime realm, simultaneously for state and non-state actors being used for positive as well as negative purposes challenging 'order at sea'. This paper is an endeavour to evaluate emerging cyber technologies potentially affecting safe navigation, and law and order within maritime domain. The research undertaken is relevant to contemporary issues which could bring important structural configuration in dealing with challenges of cyber technology advancement.

Keywords: *Maritime Security, Cyber Technologies, Hacking, Ship Security, Port Infrastructure Security, Law Enforcement at Sea.*

* The Author is Assistant Professor at School of Politics and International Relations, NUML I
** The Author is Commander Offshore 23rd Patrol Squadron, CO PMSS, Indus.

INTRODUCTION

The advent of science and technology has been playing an undeniable role in developing security, economic, political and social spheres. It is technological advancement which has led the world towards more interconnected, inter-related and interoperable international relations. Among other technology marvels, cyber connectivity has brought a revolution in contemporary world engraving deep impact on interstate relations besides other aspects of statecraft and diplomacy.

The core proposition of this study is following: The progression of cyber technologies with its wider scope has taken over maritime security considerations by affecting safe navigation, sustainable commercial and economic activities, and effective enforcement of law and order in seas and oceans making cyber security the first line of defence in international maritime environment.

The transformative quality of international relations has become increasingly encompassing with scientific innovations. It has allowed not only expansion of politics, ideologies and information, but has also increased options for policy and decision making by adding various perspectives and perceived consequences as futuristic calculations. The execution of domestic and foreign policies has accordingly become more challenging.

If technological advancement is contextualized in the backdrop of shifting security paradigm from traditional to non-traditional security in the post-Cold War era, the cyber technology emerges as an independent variable within the security discourse too with potential to redefine international relations based on spatial distinction. The maritime security has transpired a point of reference in the same time period and there occurred a shift in security discourse regarding threat perception of states as well as non-state actors and changing nature of security conceptualization and challenges in oceanic spaces.

The oceans are primary source for nutrition, connectivity and economy over which states around the world have colossal reliance. The global flows are largely dependent on maritime routes, straits, and strategic canals, while global shipping and other economic activities are the key to socioeconomic development. Political, naval, economic, commercial, and environmental diplomacy act as the backbone of statecraft. In that context, maritime security of states is getting crucial as well as its discourse is evolving with clearer conceptualization among international scholars.

Technology brings continuous progression and shifts to international relations and its praxis, particularly cyber technologies which have added perspectives and options to interstate relations. It has also threatened maritime security environment through innovative yet disruptive technologies. The undertaken research aims at evaluating emerging cyber technologies potentially affecting global economic activities, navigational safety across Sea Lines of Communication (SLOCs). Challenges to law enforcement meant establishing 'order at sea' to ensure safe and secure use of maritime domain.

This research is qualitative and analytical in nature based on explanatory research design, endeavouring to find solution of emerging challenges. The data collected for this research has used primary and secondary qualitative data making it a grounded research. This study is relevant in contemporary era of technological modernization which could bring important structural configuration in dealing with challenges of cyber technology advancement emerging in seas and oceans.

This research paper has been organized into six sections: i. Understanding Maritime Security, ii. Maritime Security: Conceptual Underpinnings, iii. Emerging Cyber Technologies and Maritime Domain, iv. Cyber Security Risks in Maritime Industry, v. Challenges for 'Order at Sea', and vi. Conclusion.

UNDERSTANDING MARITIME SECURITY

Maritime domain has emerged as the most crucial geographical realm. The whole world relies on global flows happening through oceanic spaces. More than 90 per cent trade in goods and energy takes place through oceans.[1] Maritime transport is an essential component of world supply chains and has great significance for world economy. It plays vital role in economic development of countries with a significant impact on all industries directly and indirectly. Every year billions of tonnes of cargo are loaded and unloaded at seaports. The number of containers is also swelling every year to fill up commerce and trade gaps.

Maritime activities are linked with economic growth, food security, and political stability; in other words, it is linked to every aspect of human security in the states.[2] There are

1 "Ocean Shipping and shipbuilding," *OECD,* https://www.oecd.org/ocean/topics/ocean-shipping/#:~:text=The%20main%20transport%20mode%20for,comes%20with%20opportunities%20and%20challenges.

2 Jiaqi Ge et al., "Food and Nutrition Security under Global Trade: A Relation-Driven Agent-Based Global

multiple factors like recognition of economic potential of oceans, awareness about sustainable use of maritime domain, advancement of technology and increasing significance of blue economy has brought maritime security into limelight due to resulting increase in threats and challenges in maritime domain; such as socioeconomic and environment related issues.[3]

The concept of maritime security is not de novo in its nature as safe navigation through seas has historically been assured by escorting troops, but despite existence of the concept, it is believed to be a buzzword without having any consensual definition eventually giving it a space to be discussed as challenging situation needs to be tackled. It is the concept which certainly has several dimensions. Every state and non-state actor defines security from its own perspective, but maritime security covers more dimensions than the traditional notion of sea power and use of naval forces. There are numerous definitions of maritime security that cover a wide range of areas. For instance, the International Maritime Organization (IMO) as a regulatory body under the UN relates maritime security largely with shipping;[4] whereas according to the Naval Operations Concept 2010, maritime security aims to ensure freedom of navigation, the flow of trade, and the protection of ocean resources.[5]

Furthermore, it includes protecting the maritime domain from other state actors, and transnational crimes such as drug trafficking and piracy, environmental degradation, and illegal immigration through ocean.[6] This definition combines traditional and non-traditional security threats under one umbrella and considers the concepts of maritime security and safety as one whole. It further divides maritime security into two groups. The first is individual or national security, and the other is collective security or global maritime security.[7]

Maritime security being a general and vague term has a broader spectrum under which it is described by different stakeholders and actors. An increase in maritime infrastructure

---

Trade Model," *Royal Society Open Science* 8, no. 1 (January 27, 2021): 201587, https://doi.org/10.1098/rsos.201587.

3 Malcolm Evans and Sofia Galani, *Maritime Security and the Law of the Sea,* 1st ed. (London: Edward Elgar Publishing, 2020), https://doi.org/10.4337/9781788971416.

4 International Maritime Organization, "IMO and Maritime Security: Historic background," *International Maritime Organization,* https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/IMO%20and%20Maritime%20Security%20-%20Historic%20Background.pdf. / IMO and Maritime Security - Historic Background.pdf.

5 Ibid.

6 "Naval Operations Concept *Implementing the Maritime Strategy," DOCSLIB.Org,* 2010, 35, https://www.marines.mil/Portals/1/Publications/Naval%20Operations%20Concept%202010.pdf?ver=2012-10-11-163933-953. / Naval Operations Concept 2010.pdf (marines.mil).

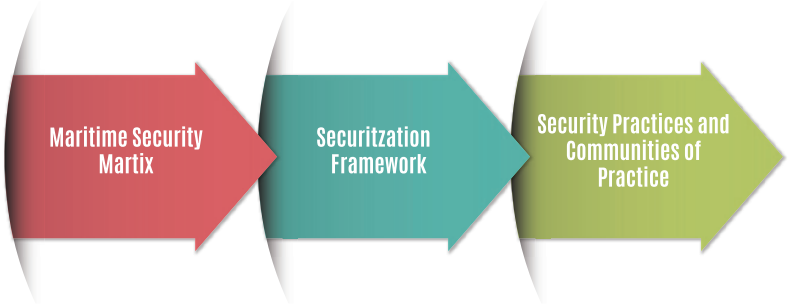
7 Ibid.

is directly proportionate to state stability and socioeconomic sustainability by creating economic opportunities, generating employment and bringing increase in GDP per capita.[8] According to the United Nations Conference on Trade and Development (UNCTAD) 2019, maritime transport plays a vital role in international trade. As a result of maritime trade, social development also happens. By and large it covers aspects of protecting vessels from seizure, sabotage, piracy, pilferage, or surprise. Since commercial value of trade through seas is backbone of international economy, shipping industry will prefer absence of outlaws and any kind of criminal or illegal activities in oceans which could hinder commercial flows, mainly from pirates or armed robbers. Therefore, it is considered to be about protection of ships both in oceans and in ports and harbours, either from malicious or accidental threats.

MARITIME SECURITY: CONCEPTUAL UNDERPINNINGS

This research has been structured on fundamental grounds established by Christian Bueger[9] which can sketchily be named as 'model of maritime security'. The three frameworks stipulated in the model provide basis for conceptual framework of this research which can be understood by the following info graph:

Info graph of Christian Bueger's Model of Maritime Security



Bueger establishes that the first framework 'maritime security matrix' is based on semiotics interpreting connection between maritime security and related concepts, and how

8 Alexandra Fratila (Adam) et al., "The Importance of Maritime Transport for Economic Growth in the European Union: A Panel Data Analysis," *Sustainability* 13, no. 14 (July 16, 2021): 7961, https://doi.org/10.3390/su13147961.

9 Christian Bueger, "What is maritime security?" *Marine Policy* 53 (2015): 160, http://dx.doi.org/10.1016/j.marpol.2014.12.005.

concepts develop inter-connectedness. This attribute enables maritime security to encompass newly explored concepts like blue economy and human resilience within an interconnected web of relations with centuries old concepts like sea power focusing more on naval power and warfare, and marine safety linked with ship and maritime installation safety.[10]

Bueger, however includes economic development and commercial growth related to ocean, particularly maritime trade and fisheries besides advancement in exploitation of offshore resources, fossil fuel, seabed mining and coastal tourism as dynamics to discuss maritime security. Food and human security are identified as the core dimensions of maritime security, and Bueger establishes a semiotic based matrix exploring interlinked concepts of maritime security. The interaction of old and new concepts enables the researchers and practitioners to develop a 'laundry list' of threats and challenges. These threats refers to all kinds of threats including interstate disputes, environment-related issues, abuse, over-exploitation or illegal use of resources, accidents or natural disasters, incidents of terrorism, piracy, trafficking or smuggling of contrabands, and illegal migrations. Thus, maritime security is made conditional with absence of these threats without addressing the core relevant questions.[11]

The second framework in that model is securitization, basically proposed by Barry Buzan and Ole Waever in which threats are constructed logically. The maritime domain, economic activities and even states are referent objects for number of existential threats; therefore, making seas and oceans securitized. They stated that securitization is possible only when actors constructing the new reality have authority, capacity and expertise to 'speak about security' and to convince the target audience about potential threat by effective politicization to further securitization of that threat.[12] Buzan and Waever talk about further process after over-politicization of existential threat as 'emergency action, and effects on inter-unit relations by breaking free of rules' for successful securitization; however, military means can be a possible, yet extraordinary and extreme way to respond to urgency of the existential threat.[13]

10 Ibid.

11 This approach sweeps every concern under the rug 'since it does neither prioritize issues, nor provides clues of how these issues are interlinked, nor outlines of how these threats can be addressed. It moreover creates enduring puzzles over which threats should be included.' The approach of not establishing clear grounds to categorize issues and to set up any criterion of threats to be included in the list is largely 'insufficient'. For detail, see Bueger, "Maritime Security?" 159.

12 Ibid, 162.

13 Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, London: Lynne Reinner, 1998), 26, 28, 42, 45, 48.

Bueger considers security practices and communities of practice as the third framework to discuss maritime security by focusing on actors involved in the process. This framework establishes its fundamentals on urgent actions taken as a result of securitization process, and includes all security practices as well as operational capabilities and technologies being used in securing maritime domain. There are five broader practices identified by Bueger in which first set of practices include maritime surveillance (through radars, sonars, satellites, or other tracking devices) under Maritime Domain Awareness (MDA) which can further use information by fusing and sharing it through appropriate data bases and service centers. Second set of practices include activities and intelligence-based operations at sea like patrols, interdictions, search and rescue, exercises, and fitness checks and inspections. Third set of practices is about law enforcement activities like reporting of crime or any unlawful activity, arresting the criminals, suspects' transfer, trials, and imprisonments.

Fourth set of practices counts on coordination among national and international stakeholders at various levels and harmonizing legal procedures, regulatory processes, mandates, strategies and implementation plans as well as impediments. Fifth and last but a significant one is a set of practices which involve naval statecraft. Its focus is on foreign policy, diplomacy, capacity building, and even warfare which is also part of foreign policy of states. Nonetheless, Bueger distributes all these practices in two categories in which first four sets of practices come under first perspective 'routine practices' while the fifth set of practices comes under second perspective of 'contentious practices and controversies around routine practices' which is aimed at studying when practices become argumentative or antagonistic. It also studies the right time to conduct certain activities without instigating controversies or how actors enforce limitations to their actions.[14]

Nonetheless, safety and security, though entirely distinct concepts, are generally translated as integral parts, and sometime used interchangeably for maritime security. Bueger describes the concept of maritime security basically in two ways 'negative' and 'positive' in which first one, the 'negative' approach is 'laundry list'. On other hand, Bueger identifies the desired 'ideal-typical end state' as positive conceptualization of the concept which talks about good or stable 'order at sea' while focusing merely on law enforcement without answering concerns regarding definition of order or whose order would be established.[15]

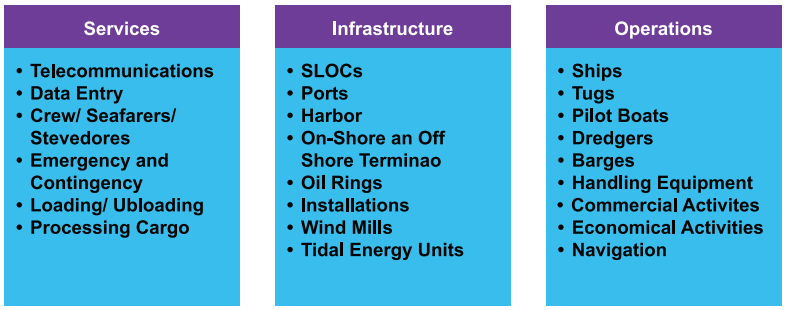
14 Bueger, "Maritime Security?" 162,163.
15 Bueger, "Maritime Security?" 159.

EMERGING CYBER TECHNOLOGIES IN THE MARITIME DOMAIN

The emerging cyber technology has emerged as a strong factor in reconfiguring power and state attributes like political communiqué, diplomatic moves, deterrence capabilities, and sustainable economic reflections like industrialization and transportation advancement. These technologies have been incorporated into maritime domain to increase maritime infrastructure and industrial efficiency. Digitalization in maritime domain involves incorporation of different types of technologies. These technologies can connect various stakeholders in different value chains.[16]

As the world is getting more reliant on modern technologies in every sphere of life, maritime realm is not an exception. The technological advancements in general and cyber space modernization in particular within maritime domain have created massive opportunities on one hand, while newer vulnerabilities are also emerging reflecting fault lines in national and international system to deal with challenges in technologically-dependent world. With evolution in concepts of globalization and integration of world economy, the concept of extended enterprise is playing a central role mainly based on technologies. Hence, it is visible that security of maritime infrastructure is essential for stability at domestic and international levels. Therefore, state and non-state actors are integrating it with several new technologies to make it more efficient. The following info graph has been structured to elaborate three major strategically important maritime cyber spaces referred as services, infrastructure, and operations where emerging technologies do play highly significant role. However, implications do occur.

Major Strategic Maritime Cyber Space



Source: The Researchers developed info graph

16 Michele Acciaro and Christa Sys, "Innovation in the Maritime Sector: Aligning Strategy with Outcomes," *Maritime Policy & Management* 47, no. 8 (November 16, 2020): 1045–63, https://doi.org/10.1080/03088839.2020.1737335.

There are currently eight dominions in maritime realm in which new technologies are emerging to bring transformation. These transformative dominions include automatic transport, robotics, artificial intelligence (AI), big data, virtual reality, augmented reality, the internet of things (IOT), cloud and edge computing, edge security, 3-D print, and additive engineering. However, overall maritime cyber technologies can be utilized into both on-shore and off-shore maritime sectors. These technologies are transforming maritime activities in all three strategic cyber spaces of services, infrastructure, and operations, simultaneously bringing massive changes to maritime transport sector.[17]

In maritime port information system, there are ten areas in which technology can bring transformation. These changes can come in a national single window system, port community system, traffic services of a vessel, terminal operating system, appoint system of gate, automated gate system, automated yard system, port road and traffic control information system, intelligent operation system, and port-hinterland information modal system.

All these systems rely on Global Positioning System (GPS), Automatic Identification System (AIS), Radio Frequency Identification (RFID), and Electronic Data Interchange (EDI) by and large besides other technologies. The data obtained from these technologies can be used for value creation using AI.[18]

Artificial Intelligence and big data can help build autonomous ships that can completely transform maritime industry. This transformation can add value in three sectors: maritime transport, improving port community system, and bringing innovation to maritime transport sector. Furthermore, big data can improve surveillance and energy efficiency through speed optimization, and route and crane planning. Moreover, predictive analytics can improve vessel performance and visual surveillance systems.[19] Using large-scale image and video analysis advancement have direct impact on maritime surveillance which can be improved significantly.

Furthermore, these advancements especially deep learning approaches can help

17 Marija Jović et al., "Digitalization in Maritime Transport and Seaports: Bibliometric, Content and Thematic Analysis," *Journal of Marine Science and Engineering* 10, no. 4 (April 1, 2022): 486, https://doi.org/10.3390/jmse10040486

18 Ziaul Haque Munim et al., "Big Data and Artificial Intelligence in the Maritime Industry: A Bibliometric Review and Future Research Directions," *Maritime Policy & Management* 47, no. 5 (July 3, 2020): 577–97, https://doi.org/10.1080/03088839.2020.1788731.

19 Ibid.

eradicate the problem of computer vision, for instance, fine-grained object recognition. This technology can help skilfully resolve the problem of maritime surveillance, which is a big challenge due to vastness of oceanic spaces.[20] Furthermore, new technological approaches are available to respond effectively to an oil spill. This technology uses a side-looking airborne radar sensor to identify oil spills in seas effectively.[21] Due to artificial intelligence, new autonomous surveillance methods are emerging that can detect objects and change.[22]

Ships use different heterogenic sensors to perform different roles. The data of these sensors can be used to monitor and improve performance of propulsion equipment and can make a future diagnosis of potential failures. These ideas are also based on the approach of using data of sensors; and through machines, vessel performance can be improved.[23] There are technologies emerging in automatic route-planning system for crane transportation. There are suggested models in which ship route and crane planning are done in advance using particle swarm optimization methods for energy consumption. There is also a method in which genetic algorithm and partial optimization swarm methods are used to get a better result.[24]

In every domain of maritime industry, there are technologies used to enhance energy conservation. There are technologies in which AI is used for speed optimization to reduce economic and environmental costs. Maritime shipping sector is responsible for 70 percent of emission of Green House gases in marine environment.[25] Therefore, it is becoming

20 Berkan Solmaz et al., "Fine-grained Recognition of Maritime Vessels and Land Vehicles by Deep Feature Embedding," *IET Computer Vision* 12, no. 8 (December 2018): 1121–32, https://doi.org/10.1049/iet-cvi.2018.5187.

21 Antonio-Javier Gallego et al., "Semantic Segmentation of SLAR Imagery with Convolutional LSTM Selectional AutoEncoders," *Remote Sensing* 11, no. 12 (June 12, 2019): 1402, https://doi.org/10.3390/rs11121402.

22 Valerio Fontana et al., "Artificial Intelligence Technologies for Maritime Surveillance Applications," in *2020 21st IEEE International Conference on Mobile Data Management (MDM)* (2020 21st IEEE International Conference on Mobile Data Management (MDM), Versailles, France: IEEE, 2020), 299–303, https://doi.org/10.1109/MDM48529.2020.00067.

23 Andrea Coraddu et al., "Machine Learning Approaches for Improving Condition-Based Maintenance of Naval Propulsion Plants," *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment* 230, no. 1 (February 2016): 136–53,\\uc0\\u8221{} {\\i{}Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment} 230, no. 1 (February 2016 https://doi.org/10.1177/1475090214540874.

24 Sanfilippo, Filippo, Lars Ivar Hatledal, Kristin Ytterstad Pettersen, and Houxiang Zhang. "A Benchmarking Framework for Control Methods of Maritime Cranes Based on the Functional Mockup Interface," *IEEE Journal of Oceanic Engineering* 43 (2018): 468-483.

25 Ibid.

significantly necessary to integrate it with AI to reduce costs and have less impact on environment. Furthermore, big data and data mining techniques are applied to find energy optimization.[26] This machine learning is also used in maritime domain to make an inventory of harmful emissions.[27] These technologies have potential to transform every sector of maritime economy, particularly commerce and trade infrastructure. On the Contrary, technological innovations are bringing efficiency at systemic level as well as causing cyber security challenges.

CYBER SECURITY AS EXISTENTIAL THREAT TO MARITIME INDUSTRY

As international maritime industry is integrating digital technology in every domain, cyber threats have also increased. In order to increase efficiency as well as speed, digitalization and emerging cyber technologies have become necessity of maritime industry.[28] Simultaneously, connectivity and reliance over intelligent devices attract cybercriminals too to exploit vulnerabilities in the maritime industry.[29] Cyber threats have the potential to disrupt maritime businesses, cause loss of finance and damage reputation, goods, environment, and legal integrity of international organizations.[30] Therefore, among 'laundry list' of non-traditional maritime security challenges, cyber technology poses existential threat with massive need to be securitized.

The World Economic Forum Global Risk Reports categorize cyber-attacks on maritime infrastructure as the fifth most considerable risk. In recent years, frequency of maritime attacks has increased a lot.[31] According to Robert Rizika, there has been a 900 percent increase in

26 Habin Lee et al., "A Decision Support System for Vessel Speed Decision in Maritime Logistics Using Weather Archive Big Data," *Computers & Operations Research* 98 (October 2018): 330–42, https://doi.org/10.1016/j.cor.2017.06.005.

27 T. Fletcher et al., "An Application of Machine Learning to Shipping Emission Inventory," *International Journal of Maritime Engineering* Vol 160, no. A4 (December 1, 2018),\\uc0\\u8221{} {\\i{}International Journal of Maritime Engineering} Vol 160, no. A4 (December 1, 2018 https://doi.org/10.3940/rina.ijme.2018.a4.500.

28 Kimberly Tam and Kevin D. Jones, "Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping," *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 147–64, https://doi.org/10.1080/23738871.2018.1513053.

29 Mohamed Amine Ben Farah et al., "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information* 13, no. 1 (January 6, 2022): 22, complemented by an analysis of key services delivered within ports. The vulnerabilities of the Global Navigation Satellite System (GNSShttps://doi.org/10.3390/info13010022.

30 Tam and Jones, "Maritime Cybersecurity Policy."

31 World Economic Forum, "The Global Risks Report 2020," Assessment (Davos: World Economic Forum, 2020).

maritime attacks from 2017 to 2020. Furthermore, in 2017 since Notpetya, a virus attack in which Maersk lost 300 million dollars, the frequency of maritime attacks has increased.[32] However, in terms of cyber security, it lags twenty years behind its contemporary sectors.

Malware attacks pose a threat to maritime infrastructure. For installing malware in a system, different devices can be used, including devices that are not capable of downloading content. Malware attacks are primarily conducted using USB.[33] It can be done in various ways, such as pre-installed malware in new USB and placing USB near maritime infrastructure at a low price. This type of incident has happened in the past using a smartphone.[34] As a result of the pre-installed virus, maritime data can be compromised. Viruses such as Stuxnet malware were introduced using similar technology.[35]

Spear-Phishing is the way of attack in which hackers use emails containing suspicious link to the targeted system. Phishing is the most common type of attack and is done to gain unauthorized access to the system. It is used to gain access to password and obtain crew and stevedores' identities for detailed target mapping. In maritime realm, numerous attacks of phishing have occurred; however, a tiny number of these attacks come to surface.[36] In similar vein, 'vishing' (voice phishing) and 'smishing' (SMS phishing) can equally be challenging for maritime activities.[37]

Introducing technologies that can jam satellite and radio signals to floating vessels and port infrastructures can hinder smooth running of maritime activities. Jamming is inexpensive method of cyber-attacks on modern ships. Ships become a specific target for jamming because of interference into GPS since ships are far away from source of signals usually resulting into weakening of signals; therefore, jamming the signal through concentrated noise becomes an

32 MI News Network, "Maritime Cyber-attacks Increase By 900% In Three Years," *Marine Insight* (blog), July 20, 2020, https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/.

33 Jacob Mackiewicz et al., "Mouse Trap: Exploiting Firmware Updates in {USB} Peripherals," *USENIX,* 2014, https://www.usenix.org/conference/woot14/workshop-program/presentation/maskiewicz.

34 Aatif Sulleyman, "If You Have an Android, You Need to Read This," *The Independent,* March 14, 2017, https://www.independent.co.uk/tech/android-malware-phones-infected-samsung-galalaxy-s7-nexus-5x-models-before-sale-a7626726.html

35 Danny Palmer, "IBM Warns of Malware on USB Drives Shipped to Customers," *ZDNet,* May 02, 2017, https://www.zdnet.com/article/ibm-warns-of-malware-on-usb-drives-shipped-to-customers/.

36 Ben Farah et al., "Cyber Security in the Maritime Industry."complemented by an analysis of key services delivered within ports. The vulnerabilities of the Global Navigation Satellite System (GNSS)

37 Ben Farah et al., "Cyber Security in the Maritime Industry."complemented by an analysis of key services delivered within ports. The vulnerabilities of the Global Navigation Satellite System (GNSS)

easy target.[38]

Denial of services vulnerability has become another significant maritime cyber security issue because modern ships rely more on sensor data to make decisions.[39] Therefore, they become more vulnerable to DOS attacks. These attacks can damage sensors or transmitters. However, in some cases, it can also physically damage the ship. This attack can also be used tocreate an explosion in the ship. In modern ships, sensors' data is used to measure and maintain the fuel. Changing data of fuel through network attacks can effectively damage ships.[40]

Spoofing is another threat that exists in maritime cyber domain. It is more complicated than jamming. In this attack, ship's GPS is hacked to change its location. Due to spoofing, misdirection becomes unnoticeable. New technologies are emerging in which crewless ships use GPS to navigate through ocean. They use Artificial Potential Field Method to plan ship's route. GPS spoofing can significantly impact the path planning for un-manned ships.[41] In 2017, an incident of mass spoofing through GPS took place in Black Sea in which a tanker ATRIA reported that its GPS was showing it 20 nautical miles away at Gelendzhik Airport instead of its correct location off-Russian port of Novorossiysk. When AIS was used to trace, at least 20 ships were found at that location. It was perceived as part of Russia's e-warfare.[42]

38 Alan Grant et al., "GPS Jamming and the Impact on Maritime Navigation," *Journal of Navigation* 62, no. 2 (April 2009): 173–87, https://doi.org/10.1017/S0373463308005213.

39 Zhang Yingjun et al., "Shipping Containers of Dangerous Goods Condition Monitoring System Based on Wireless Sensor Network," *INC2010: 6th International Conference on Networked Computing,* 2010.

40 "Safety & Shipping Review," *Allianz Global Corporate & Specialty,* 2016, https://www.agcs.allianz.com/news-and-insights/reports/shipping-safety.html

41 Jia Wang et al., "Impacts of GPS Spoofing on Path Planning of Unmanned Surface Ships," *Electronics* 11, no. 5 (March 4, 2022): 801, https://doi.org/10.3390/electronics11050801.

42 Gary C. Kessler, "GNSS/AIS Spoofing: Issues in Maritime Cyber Security," Maritime Cyber Security 2021 virtual event, June 25, 2021, https://www.youtube.com/watch?v=0YAgReDku9k. "GNSS/AIS Spoofing: Issues in Maritime CyberSecurity" by Gary C. Kessler - YouTube.

Source: Gary C. Kessler's Presentation[43]

Similar kind of GPS related Spoofing incidents took place in different parts of Mediterranean during 2018, i.e. Cyprus (March and November), Haifa (November), Port Said and Suez Canal (March, July, October, November) and Eastern Mediterranean Region (March to May);[44] and these were not lone cyber-attacks or GPS Spoofing issues. Following years have witnessed increased frequency of such incidents.

A malware attack took place on the South Korean oil drilling rig in 2010. Although maritime infrastructure was not a direct target, a computer in the system transferred the malware to the entire system. Since it could infect the blowout-preventer system leading to an explosion if it was working, the entire system had to be shut down for 19 days. Stuxnet is another example of malware that is capable of doing physical damage. It was used to attack the Iranian nuclear facilities. The same malware was found in maritime chevron facility.[45]

Furthermore, another example of public maritime hacking was conducted in Iran in 2010 when Iran Shipping Line was targeted. Due to this attack, it lost millions of dollars, and cargo was never recovered. Similarly, pirates also use hackers to get information about the vessels and other details.[46] In 2018, the subsidiary company of COSCO shipping Line

43 Ibid, at 17:37/42:59.
44 Kessler's Presentation.
45 Gary C Kessler and Steven D Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers,* 2020.
46 Ibid., 34

became a victim of cyber-attacks. A ransom ware attack shut down its IT system for days. In 2019, hackers used Ryuk ransom ware to shut down the multiple port operation for thirty days. In 2020, companies such as Carnival, CMA CGM Group, Garmin, Hurtigruten, Port of Kennewick, and Toll became victims of cyber ransom ware.[47]

Hence, there are multiple cyber threats to maritime commerce and economic infrastructure, making it very challenging to world economy as well as challenging to 'order at sea'. An integrated system that uses big data and artificial intelligence increases system's complexity and becomes prone to cyber security attacks. Following Bueger's maritime security model, the analysis has supported through evidence that maritime commerce, trade and other economic activities are referent object vulnerable to cyber security breach by malicious intentions and accidents. Since the vector of cyber security challenges is quite broad, whatever the nature of challenge would be there, that is an existential threat due to which emerging cyber technologies need to be securitized. Fine grained analysis establishes that such threats do disrupt 'order at sea' and make law enforcement a larger-than-life issue for the states. However, developing states are the ones with possibility of getting affected more than the developed ones due to their redundant strategies.

CHALLENGES FOR 'ORDER AT SEA'

Maritime cyber security has become a significant issue in maritime domain. It has the potential to disrupt order at sea. According to Allianz Risk Barometer 2019, cyber security is a central problem for maritime businesses. In 2014, maritime businesses lost 458 billion dollars due to cybercrimes; in 2019, losses increased to 600 billion dollars. Cyber-crimes pose a significant risk to the world trade which is overchallengingly dependent on sea.[48]

The attacks on ships can have harmful consequences for economic losses to maritime industry. These attacks can have dire consequences for human life and marine environment. In early 2021, Maersk vessels lost 260 containers due to a malfunction in its propulsion system. The Maersk incident was not isolated one.[49] Rather other incidents of similar nature do happen with other ship liners too. According to the World Shipping Council, on average,

47 William Loomis et al., "Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity" (Washigton Dc: Atlantic Council, 2021), https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Raising-the-Colors-FINAL-.pdf.

48 Real Harris, News and Analysis, Oceans Technologies Group, *"How Big a Problem Is Maritime Cyber Security?"* November 25, 2019, https://www.oceantg.com/blog/the-problem-of-maritime-cyber-security/

49 Loomis et al., "Raising the Colors."

annually 1382 containers have been lost in oceans in last ten years.[50]

A notable catastrophic incident of the maritime trade disruption happened in Suez Canal in March 2021, where a container ship ran aground in the canal. That closure of Suez incident caused significant damage to maritime trade and consequently, 9.6 billion dollars of goods were stuck. This vessel was 1300 feet long and had 22100 TEU of goods on board.[51] It took six days and a considerable effort using different means to clear this blockade. However, the supply chain disruption caused by this ship took 60 days to clear because world ports were clogged due to that incident.[52]

Though investigation of the incident has reflected non-involvement of any cyber-attack, but that can be a precursor of further incident by using disruptive technologies available such as hacking of the steering and navigation system. The Internet Protocol Network used in steering and navigation system is not made to provide safety against cyber-attacks.[53] These systems are connected to serial bus network, which plays a significant role in ships operation because of supervisor control and data acquisition system. Even the electric system for locks in Panama Canal poses a significant risk to disruption of maritime trade by belligerent actors.[54]

Malacca Strait is also vulnerable to cyber security attacks. That maritime bottleneck is like motor nerve for Chinese and other East Asian countries' trade. Blockade of such chokepoints due to cyber-attacks can impact trade through these routes.[55] Furthermore, cyber-attacks around Bab-el-Mandeb and Gulf of Aden are also serious concerns because nations around these choke points are least prepared for such attacks. In the latest evaluation of risk exposure and ranking, these nations were at 27 out of 27 countries at risk of cyber-crimes.

These cyber-crimes are not limited only to trade and commercial activities. Every off-shore facility and vessel has certain challenges to face or cause, specifically the ones involved in

50 Ibid., 10

51 Jade Man-yin Lee and Eugene Yin-cheung Wong, "Suez Canal Blockage: An Analysis of Legal Impact, Risks and Liabilities to the Global Supply Chain," ed. P. Khvedelidze, B. Gechbaia, and K. Goletiani, *MATEC Web of Conferences* 339 (2021): 01019, https://doi.org/10.1051/matecconf/202133901019

52 Ibid.

53 Loomis et al., "Raising the Colors." 25

54 Ibid.,35

55 Sheldon W. Simon, "Safety and Security in the Malacca Straits: The Limits of Collaboration," *Asian Security* 7, no. 1 (February 28, 2011): 27–43, https://doi.org/10.1080/14799855.2011.548208.

illegal activities like piracy, smuggling, trafficking, illegal and unregulated fishing, poaching of fisheries, seafood and other marine resources. There are several ghost or dark vessels in oceanic spaces all the time. Those vessels can hide themselves by turning off their AIS or can spoof identification or location information making their presence difficult to be surveyed or detected. The impact of such occurrences is seen either in the form of defective data as there would be 'gaps in data, monitoring and accountability,'[56] or according to Paul Woods, making potential, already 'fragile marine areas' detectable for maritime outlaws through analysis or leakage of defective data.[57] To counter such kind of emerging cyber threats and challenges in the maritime domain, Synthetic Aperture Radar (SAR) technology is used which works effectively even during dark, cloudy or stormy weather, identifying all ghost or dark vessels.[58]

Radar (SAR) Detections (February 2022 and May 2022)

Source: Global Fishing Watch[59]

Maritime cyber advancements, mechanization and digitalization have brought another dimension to maritime security studies in which emergence of one non-traditional threat creates conducive environment for further threats. A significant consideration is increase in maritime cyber-crimes after the world was engulfed by Covid-19 pandemic which was an unprecedented non-traditional security issue. During lockdown, cyber-attacks increased

56 The Editorial Team, Safety4Seas, "Map reveals undetected dark fishing vessels," June 09, 2022, accessed July 09, 2022, https://safety4sea.com/map-reveals-undetected-dark-fishing-vessels/. / Map reveals undetected dark fishing vessels - SAFETY4SEA.

57 Ibid.

58 Ibid.

59 "Global Radar Detections (SAR)," "*Global Fishing Watch,*" accessed on July 10, 2022, GFW | Fishing activity (globalfishingwatch.org).

by 400 per cent since people indulged more into cyber related activities.[60] Nonetheless, emerging cyber technologies have endangered maritime security and maintaining 'order at sea' has become significantly challenging task.

The International Maritime Organization (IMO) has responded to growing cyber security threats through resolution 428 (98). In addition, this resolution has been complemented by other regulations, such as those developed by the International Baltic Council. These guidelines ensure ships' security by incorporating cyber risk management into the existing safety management system. All ships needed to follow the guidelines set in the IMO resolution to travel worldwide.[61]

In order to facilitate compliance with the guidelines set in the IMO resolution, BIMCO and other regional organizations have developed the blueprints which ship owners can follow. The US government began to address the shortfall in maritime cyber security by releasing a national security plan in 2020. However, current international legal framework is inadequate to deal with these threats. There is a need for further steps to reform international legal framework comprehensively with the help of state and non-state actors to reduce negative implications of emerging cyber technologies in maritime domain effectively.[62] There was some compliance on part of ship owners; however, it failed to reduce cyber-attacks in maritime industry. Even after implementation of that regulation, a 400 percent increase was noticed in cyber security, and hack attempts on maritime industry worldwide increasing cyber vulnerability.[63]

Maritime cyber security, like other non-traditional maritime security concerns, requires legal cover which comes from international laws and regulatory authorities. National laws and regulations are formulated in the light of international frameworks. The legislation and strategic measures are adopted by the law enforcement agencies which are responsible for maintaining 'order a sea' through efficient constabulary and effective enforcement of policies

60 Mission Secure, *" Current Threats to Maritime Security: A Prime Target for Cyber Adversaries,"* accessed on June 26, 2022, https://www.missionsecure.com/blog/maritime-a-prime-target-for-cyber-adversaries. / Current Threats to Maritime Security: A Prime Target for Adversaries (missionsecure.com).

61 International Maritime Organization, *"Maritime Cyber Ris"*, 2021,https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

62 Md Saiful Karim, "Maritime Cybersecurity and the IMO Legal Instruments: Sluggish Response to an Escalating Threat?," *Marine Policy* 143 (September 2022): 105138, https://doi.org/10.1016/j.marpol.2022.105138.

63 Sabba Manyara, The Asset, "Rising Cyber Exposure in Asia Maritime Shipping," 2022, https://theasset.com/article/45794/rising-cyber-exposure-in-asia-maritime-shipping.

and laws. The praxis of maritime cyber security makes the third framework mentioned by Bueger in his model a significant part of maritime security. There are gaps in the area of maritime cyber security in majority of states due to absence of enabling environment for cyber security policies and redundancies in domain of relevant training to deal with potential cyber threats. Shipping lines, ports and terminals do have their own cyber security framework but this area requires intense laws and policy formulation to ensure effective 'order at sea'.

CONCLUSION AND RECOMMENDATIONS

Safety and security of maritime environment is a globally shared responsibility as any individual state is not capable enough to ensure maritime security across the oceans. Increased opportunities and resulting challenges occurring due to cyber technologies need effective constabulary role and regulatory processes to enhance 'order at sea' and overall ocean governance. This research has examined that emerging cyber technologies in maritime domain particularly used in economic and commercial activities including global flows, maritime transportation, energy pipelines and terminals, internet connectivity, fishing, cargo terminals and equipment, etc. have made number of practices regarding maritime security ineffective and deficient. The level of preparedness both on ships and in ports and harbours are at risk of massive losses of life, economy, commerce, and environment.

There are emerging technologies which can become disruptive or detrimental to maritime security. The potential threats can surface anywhere, any time for on-shore and off-shore entity and personnel, i.e. any kind of floating vessel, any member of crew, seafarers, stevedores, operators or other personnel, cargo, ports and terminals. Effective maritime cyber security involves protection of Information Technology (IT), Operational Technology (OT), functional information and data of nautical charts from unauthorized access, manipulation, disruption and denial. In general, cyber-attacks are considered as incidents using a cyber-vector towards a cyber-target. There is a need to carve out a strategy with clearly defined contours to protect maritime environment, trade, commerce and other economic activities from harmful impact of emerging technologies.

Cyber security of vessels, ports, and other parts of maritime transport system needs to be taken seriously, and 'sick' and 'healthy' entities should be identified for appropriate action. The strategy should have protocols by the authorities for vessels and crew/personnel to be checked for cyber infections before they connect to any public dock or port's network. In case of detected or suspected infections, the subject should be quarantined and supported by

cyber experts to prevent port and terminals' digital castle from any harm.

It may be noted that till date many infrastructures handling sea or harbor operations are still not connected with cyber technology due to overwhelming desire of the state and other stakeholders to prevent cyber threats and challenging situations involving protection of IT systems being used at all three strategic cyber spaces of services, infrastructures, and operations. Cyber-attacks may lead to misinformation about personnel on ferry ship or may cause delay in sailing of vessel. It can also advance or reduce functioning of sophisticated sensors, instruments, networks etc. Maritime cyber threats may lead to cyber terrorists having control of autonomous vehicles at a port facility and use the same to damage equipment. Further, a ship may get its navigational system hacked and end up grounding or colliding. If a ship is carrying hazardous material it can become more prone to cyber terrorism where sensors or gauges are deliberately altered to end up in marine disaster. Resultantly, cyber threats can lead to imbalance in commerce activity of target country or company.

Ultimately, all cyber-attacks have a physical target, whether directly or indirectly. Consequently, IMO has issued guide lines for member states to cater for cyber maritime threat. It will help to protect maritime environment, trade, commerce and other economic activities from harmful impact of emerging technologies. Member states have to formulate own strategies in order to prevent cyber-attacks and/or to formulate mitigation strategies to bring the system back online. The most significant fundamental step is to educate individuals and enterprises about existential threat of maritime cyber security, and from that point onwards, consensual laws and strategies could be devised at international and national levels. A firm ground for enforcement mechanisms supported by laws and regulations will ensure stable 'order at sea' and the role of law enforcement agencies will become more robust and effective.