Editor in Chief
Capt. (TÜR-N) Mustafa POYRAZ

OPR.
Cdr. (TÜR-N) Mehmet Deniz ÇETİKLİ

Published By

Maritime Security Centre Of Excellence (MARSEC COE)

Academic Advisor:
Prof. Dr. Giray SADIK

Cover Designer:
Cdr. (TÜR-N) Mehmet Deniz ÇETİKLİ

MARITIME SECURITY CENTRE OF EXCELLENCE
"Working Together for Maritime Security"

Address: Deniz Güvenliği Mükemmeliyet Merkezi Komutanlığı, Milli Savunma Üniversitesi
Yerleşkesi, 34330, Yenilevent - İstanbul / TÜRKİYE

Phone: +90 212 398 01 00 (5885)

E-Mail: info@marseccoe.org

Printed by
Çözüm Baskı Merkezi Ticaret Limited Şirketi
Emniyetevleri Mahallesi Güvercin Sokak No:7/1 KAĞITHANE / İSTANBUL

Phone: (0212) 281 49 48 **Gsm:** +90 543 297 43 59

This document, a product of the Maritime Security Centre of Excellence (MARSEC COE), is intended solely for the recipient's use. Any unauthorized reproduction, distribution, or disclosure to third parties without the explicit consent of MARSEC COE is strictly prohibited. The views presented in the articles of this paper are those of the author alone and do not represent the opinions or policies of NATO or MARSEC COE. The Centre is not liable for any loss or harm arising from the use of the information contained in this paper and does not endorse or take responsibility for the content of external sources, including websites referenced in this paper.

MARITIME SECURITY CENTRE OF EXCELLENCE

Working Together for Maritime Security

3rd MARITIME SECURITY CONFERENCE PROCEEDINGS

MARITIME SECURITY IN THE SCOPE OF NATO's NEW STRATEGIC CONCEPT

Disclaimer: This is a product of the MARITIME SECURITY CENTRE OF EXCELLENCE (MARSEC COE). The views presented in the articles of this conference proceedings are those of the authors alone, and they do not represent the opinions or policies of NATO or MARSEC COE. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this conference proceedings and is not responsible for the content of the external sources, including external websites referenced in this paper.

DIRECTOR’s REMARKS

Dear Readers,

As the Director of the Maritime Security Centre of Excellence, I am delighted to present the proceedings of our conference. The theme of our conference, “Maritime Security in the Scope of NATO’s New Strategic Concept,” was timely and relevant, considering the dramatic shifts in the global security environment defined by strategic competition.

Our conference provided a platform for insightful debates among multi-stakeholder experts from academia, military, and private sectors. We had speakers and participants from 19 different countries, bringing a diverse set of expertise to the table. The discussions and debates were rich, enlightening, and thought-provoking.

The conference highlighted the importance of maritime security in times of peace, crisis, and conflict. It underscored the need for a seamless nexus between our maritime forces and cyber, digital, and space domains as well as the critical infrastructures that host our naval assets. The notion of ‘continuum of seas’ was emphasized, advocating for a holistic approach to maritime security.

I would like to express my gratitude to MARSEC COE team for their unwavering support throughout the conference. I also extend my thanks to Moderators and Lecturers for their invaluable contributions.

The proceedings published in this edited volume reflect the insightful debates that took place during the conference. I encourage you to read these papers as they represent diverse perspectives on maritime security.
Best Regards,

Mehmet Cengiz EKREN
Captain (TUR-N)
Director of MARSEC COE

3rd MARITIME SECURITY CONFERENCE PROCEEDINGS

MARITIME SECURITY IN THE SCOPE OF NATO's NEW STRATEGIC CONCEPT

-2024-

Table of Contents

EXECUTIVE SUMMARY

I. Introduction 'Conference Theme'

NATO Strategic Concept 2022, adopted in Madrid, has set an ambitious roadmap for maritime defense planners and experts. In the face of significant shifts and challenges in the global security environment, ensuring maritime security is paramount for the promotion of peace and prosperity for the Allies. NATO commits to strengthening alliance posture and situational awareness to deter and defend all threats in the maritime domain. To this end, MARSEC COE gathered the 3rd Maritime Security Conference as a good instrument focusing on "Maritime Security in the Scope of NATO's New Strategic Concept".

II. Overview of the conference panels

a. Panel 1: New Trends in Leveraging Unmanned Systems for Maritime Security

Autonomous shipping has advantages in terms of safety and security, but it also poses risks and dangers. These include concerns around human factors, collision avoidance, technical failures, cybersecurity threats, reliability of remote control, and environmental protection. The problems at hand cannot be solved by relying solely on existing norms, standards, rules, and regulations, as they are insufficient to address them adequately.

(1) Navigating Regulatory Challenges: Ensuring Safety and Security in MASS

Maritime Autonomous Surface Ships (MASS/autonomous ships), also referred to as unmannedships, are rapidly advancing technologies. These advancing technologies hold potential benefits such as increased efficiency and lower operational costs. At the same time, they also present a plethora of safety and security concerns such as including but not limited to human factors, collision avoidance, technical failures, and cybersecurity threats. These issues raise questions about the standards and norms to be implemented. When establishing a legal and regulatory framework for autonomous ships, timely insights are necessary to address these multi-domain challenges of unmanned systems for maritime safety and security.

(2) Usage of Maritime Unmanned Systems in Support of Maritime Security Operations

Maritime unmanned systems (MUS) have been used to collect intelligence, surveillance, and reconnaissance and have enhanced maritime situational awareness by providing more accurate and sustainable data. Unmanned systems' adaptability, versatility, and cost-effectiveness have been indispensable to successful maritime security operations. MARSEC COE's draft concept, *Usage of Maritime Unmanned Systems in Support of Maritime Security Operations*, focuses on how, in what contexts, and to what extent MUS can be employed in Maritime Security Operations (MSO) and its seven MSO tasks:

Protection of Critical Infrastructure, Supporting Maritime Counterterrorism, Fighting Against the Proliferation of Weapons of Mass Destruction, Contributing to Maritime Security Capacity Building, Supporting Maritime Situational Awareness, Upholding Freedom of Navigation, and Maritime Interdiction Operations.

(3) Effectiveness Analysis of Unmanned Surface Vehicles in Littoral Waters

Unmanned systems will change the nature of the future battleground, and Unmanned Surface Vehicles (USVs) are an important part of this change as they have already been in use for port protection and maritime surveillance. The effectiveness of USVs in littoral waters with different platform types, sensors, and weapon combinations in a wide variety of different scenarios such as Anti Surface/Submarine/Air warfare, port security, and law enforcement duties is analyzed in discussions.

b. Panel 2: NATO's New Strategic Concept and Implications for Maritime Security

In the context of the transforming strategic landscape and NATO's New Strategic Concept, to maintain deterrence and defense, a substantial and persistent presence of maritime forces at sea has become more important. This panel puts forward this timely call for the growing importance of maritime security by elaborating on the critical implications in three in-depth analyses presented and their findings summarized in the below sub-section. Overall, they highlight that it is essential for maritime forces to remain ready, resilient, responsive, usable, deployable, and interoperable across the board and at all times and regions of the Alliance and beyond including the Indo-Pacific.

(1) NATO Strategic Concept and NATO Defense Plans and the Maritime Domain

In the past, NATO's Strategic Concept defined its military strategy. However, the 2010 NATO Strategic Concept did not facilitate the development of a new military strategy. As a result, the military strategy and Defence Planning Assumptions (DPA) were developed first, and many of the themes which are in those documents havebeen refined and incorporated into the Strategic Concept. Potential implications of the Strategic Concept for maritime security are expanded by highlighting that whilst implementing the Strategic Concept, maritime forces will have asalient role both in SACEUR's Strategic Directive and in the SACEUR Area-Wide Strategic Plan, namely SASP. It is also anticipated that the deterrence and defense function of maritime forces in Domain-Specific Plans and the three Regional Plans would be duly elaborated. The need for a comprehensive strategy for the Mediterranean and questions about how this challenge will be addressed in NATO's Regional Plans is emphasized.

(2) Implications of the NATO's New Strategic Concept in the Black Sea and Other Seas

The question of how the United Nations Convention on the Law of the Sea and the 1936 Montreux Convention contribute to this NATO rules-based order in the Black Sea and other seas of conflicts, like the Mediterranean, the Baltic Sea, the South China Sea, and the Gulf of Mexico is examined in the conference.

From a regional perspective of the Black Sea, the need for a balanced approach that respects the Montreux Convention's provisions as part of international law, advocating for a Montreux-friendly arrangement that complements NATO's security efforts in the wider Black Sea region, including the maritime domain is expressed by the speakers.

(3) The Indo-Pacific Security Importance for the Alliance

The increasing importance of the Indo-Pacific region for the United States and other NATO Allies is highlighted. Attendance of the 4 non-member guests (Australia, New Zealand, Japan, and the Republic of Korea) from the region at the 2022 NATO Madrid Summit supports this idea: Another document indicating Allied growing concern about the region could be the 2022 NATO strategic Foresight Perspectives Report on the Indo-Pacific, where the rise of China was recognized as a growing threat. Putting forward the experts' prediction that future wars will be for raw materials and the most valuable raw materials lie at the bottom of the Pacific Ocean.

c. Panel 3: NATO's Role and Legal Aspects in Maritime Critical Infrastructure Protection

In the aftermath of the Russia-Ukraine war, maritime security has become increasingly significant, with cybersecurity developments making it a top priority for states and alliances like NATO. This panel focuses on the protection, safety, and security of maritime critical infrastructure, which is primarily a national responsibility.

(1) Maritime Critical Infrastructure Protection in a Changing Security Environment

Maritime Critical Infrastructure (MCI) and Critical Energy Infrastructure (CEI) are vital for the functioning of societies, economies, and countries. In this vein, the maritime domain is vulnerable to various types of threats such as physical, cyber, and hybrid, which can affect multiple areas simultaneously. The concept of critical infrastructure, the role of MCI/CEI, the risks faced by MCI/CEI, and the steps to be taken to ensure maritime resilience are the topics to discuss Maritime Critical Infrastructure Protection in a changing security environment.

(2) Offshore Critical Energy Infrastructure: A Maritime Security Perspective

Ongoing energy transitions in NATO countries come with the development of energy interconnections. These interconnections are critical links not only for the NATO members but also for connecting the Allies with non-NATO major energy production areas globally. Accordingly, the need to map the dependency of NATO countries on these offshore critical energy infrastructures and asses their vulnerabilities is addressed.

(3) Security and Protection of Critical Undersea Infrastructures: The Italian Perspective

Today's economies are utterly reliant on the global information technology infrastructure with 99 percent of communications moving through undersea cables, most of which are lacking even basic defenses. Therefore, stepping into the legal aspect, it is essential to define a regulatory framework, as for air and space traffic control, in order to enable the coordination, monitoring, and control of underwater activities, and to achieve persistent and extensive underwater situational awareness (UWSA).

(4) A Short Note on the Legal Aspects of the Protection of Critical Maritime Infrastructure and the Role of NATO

The existing legal framework for protecting Critical Maritime Infrastructure (CMI) is deemed inadequate in the face of evolving threats. The Nord Stream incident served as a catalyst for NATO to increase patrols and establish a Critical Undersea Infrastructure Coordination Cell for better collaboration. The analysis emphasizes the need for NATO to work closely with private partners, like the EU, invest in maritime capacity building, and take proactive measures to safeguard CMI against both willful attacks and emerging threats. The continuous growth and dependence on CMI necessitate robust and comprehensive efforts to ensure its protection.NATO members' legal resilience is necessary to protect CMI. Legal resilience combined with state-of-the-art technology, such as unmanned systems, would enable NATO members to respond to threats to CMI more effectively.

(5) Legal Aspects of the Protection of Submarine Communication Cables: A Primer

Given the fundamental importance of submarine communication cables, the protection of modern global communication from man-made threats is crucial. How international legal regime for protecting and managing submarine cables has remained largely unchanged since the 19th century. And also how the contemporary law of the sea's limited approach to the matter, complicates the protection of this maritime critical infrastructure in the face of emerging threats.

d. Panel 4: Holistic Perspectives on Maritime Security Challenges: Cybersecurity and Beyond

Risks from Disruptive Impact Events (DIE) can have far-reaching implications for the NATO Allies and therefore for the Alliance. The maritime domain is no exception, and a compromise at the logical and physical layers of cyberspace may produce unwanted effects on combat systems, navigation, command and control systems, computers, communications, and thus putting national and Allied personnel at risk and potentially causing significant physical damage. Based on their below summarized comprehensive research findings, the authors of this panel aim to offer timely insights to address these multi-domain challenges that can be considered for future maritime capability building that aligns with the new NATO strategic concept.

(1) Cyber Threat Intelligence: Mitigating Risks to Maritime Security

In today's modern military operations, a cyberspace ecosystem is an essential part of the overall strategy. This means, however, that not only are there new opportunities, but also new vulnerabilities and threats, and the maritime domain is no exception The severity of the threat is recognized and reflected in NATO's new strategic concept published on 29 June 2022, which emphasizes the need for increased focus on cyberspace security and recognizes cyber threats as an integral part of modern multi-domain operations. To address this threat, NATO is taking a multi-pronged approach that includes developing cyber capabilities, promoting information sharing and collaboration, and investing in research and development. One critical aspect of this approach, the authors claim, is cyber threat intelligence (CTI), which involves collecting and analyzing information about potential threats to identify and mitigate risks. In their article, the authors analyze NATO's strategic concept to determine how maritime-focused CTI guidance could be fostered and used effectively for the Alliance.

(2) Disruptive Impacts on Maritime Industrial Base Supply Chain and Naval Readiness

The effectiveness of the Maritime Industrial Base (MBE) can be diminished by severe weather events, targeted degradation of Critical Infrastructure (CI), public health crisis, or any combination thereof. To address these challenges, one of the proposals is an approach and methodology to create a valid representation of a maritime System of Systems (SoS), where dependencies must be systematically elicited from human assets with direct working knowledge of the dependencies across dependency functions, including cyber, equipment, materials, labor, fuel, and chain of command.

III. Key Findings and Recommendations

a. Collaborative Approach to Maritime Challenges

The insights gathered from the 3rd Maritime Security Conference indicate that the emerging threats in today's intricate era are too substantial for any single state to confront alone. This underscores the necessity for a cooperative approach to tackle contemporary maritime challenges.

b. Strengthening Maritime Situational Awareness

In order to fulfill the objectives of the new NATO Strategic Concept concerning maritime security, there is a need to bolster maritime situational awareness. This will ensure that Allied navies are resilient and prepared to respond effectively against a spectrum of escalating threats, including those posed by emerging disruptive technologies.

c. Holistic Approach to Maritime Critical Infrastructure Protection

The safeguarding of maritime critical infrastructure necessitates a comprehensive approach. This includes but is not limited to, addressing challenges presented by hybrid warfare, maritime terrorism, and large-scale pollution.

d. Technological Advancements and Legal Frameworks

The growing use of technology further challenges the effectiveness of the existing legal frameworks designed for the protection of maritime critical infrastructures.

e. Acquisition of New Capabilities and Technological Development

There is an urgent need for navies to acquire new capabilities and to foster a new model of technology development in collaboration with industry and academia. This will ensure that they are equipped to handle the evolving maritime security landscape.

IV. Conclusion

The security of the seas is of paramount importance, as it not only safeguards NATO's Area of Responsibility but also upholds the shared interests and values that drive the Alliance. In the face of intensifying strategic competition, it is crucial to 'enhance global awareness and reach to deter, defend, contest, and deny across all domains and directions, in line with a 360-degree approach,' as stipulated by the New NATO Strategic Concept. The conference provided a timely platform to reflect on these significant issues and their impact on maritime security in light of recent developments. The discussions underscored the necessity of maintaining a seamless connection between maritime forces and cyber, digital, and space domains, as well as the critical infrastructures that host naval assets. This necessitates the implementation of the concept of 'continuum of seas', thereby avoiding compartmentalization. A holistic approach is, therefore, of utmost importance for NATO Allies and partners.

As the Academic Advisor of the 3rd Maritime Security Conference, gratitude is extended to the leadership of MARSEC COE for their support throughout the conference. The conference organizers are thankful for the guidance provided by Defense Planning and Project Management Director R. Adm. Refik Levent Tezcan (TUR N) who served as a keynote speaker in the opening session and remained actively engaged until the end of the conference. The conference successfully brought together speakers and participants from 19 different countries, with a diverse set of expertise spanning military, public-private sectors, and academia. Reflecting on their insightful debates, the conference proceedings are published in this edited volume. The authors of the conference proceedings have always been encouraged to be free in their analyses, so the views expressed in their papers should be considered as the perspectives of their respective authors only.

Prof. Dr. Giray SADIK
Academic Advisor

‘NAVIGATING REGULATORY CHALLENGES: ENSURING SAFETY AND SECURITY IN MARITIME AUTONOMOUS SURFACE SHIPS (MASS)’

Mustafa Yilmaz
DEHUKAM

I. Maritime Autonomous Surface Ships (MASS)

a. Definition

There is still no universally accepted term or title to denominate these new generation ships. Instead of the term ‘Maritime Autonomous Surface Ship’ (MASS)[1] the terms ‘unmanned ship’, ‘autonomous unmanned ship’, ‘uncrewed/crewless ship’, ‘self-steering ship’, ‘highly automated ship’ and ‘smart ship’ are also used. Following the International Maritime Organization's (IMO) introduction of MASS as a more inclusive term, albeit it caused some controversy initially, it has now been widely accepted and embraced.

The IMO defines MASS as “*a ship which, to a varying degree, can operate independently of human interaction”*. It refers to a ship with some form of autonomy that allows it to perform a set of defined operations and to navigate and be steered with no or minimal crew on board[2]. The IMO has identified four levels of autonomy, from ships with automated processes and decision support (MASS-1) to fully autonomous ships where the ship’s control system makes decisions and determines its movements on its own (MASS-4).

MASS-1 (Degree One): A ship with automated processes and decision support Seafarers are constantly on board to operate and supervise some systems and functions on MASS-1. Although some operations are performed automatically, seafarers are ready to take command of the ship at any time[3]. MASS-1 is the autonomous ship type with the closest configuration system to the conventional ships, regularly under crew management on board. In other words, the actions taken by the MASS-1’s control system are perpetually open to the intervention of the crew on board.

MASS-2 (Degree Two): Remotely controlled ship with seafarers on board. MASS-2 is an autonomous ship remotely controlled and operated from another location, namely the control centre. The seafarers are on board to take over the ship’s command at any time, whereas the control centre plays the leading role in the control and management of the ship.

MASS-3 (Degree Three): Remotely controlled ship without seafarers on board. MASS-3, also known as the remotely controlled ship, is an autonomous ship type with no seafarer on board responsible for the ship’s

[1] This work uses both the term ‘autonomous ship’ and the abbreviation ‘MASS’, referring to the IMO’s term ‘Maritime Autonomous Surface Ship’.

[2] RØDSETH, Ørnulf - NORDAHL, Håvard: “Definitions for Autonomous Merchant Ships”, NFAS (*Norwegian Forum for Autonomous Ships*), Trondheim 2017, p. 7.

[3] IMO, Takes First Steps.

navigation and management[4]. The ship is controlled and operated by the operators in the control centre. The transition to automation on ships is not a new phenomenon. Be that as it may, what makes MASS-3 and MASS-4 unprecedented is that the conventional captain's bridge is not involved in the navigation and management of the ship. The ship's bridge, therefore, loses its vital significance and becomes redundant to such an extent that it gives full rein to the control centre in MASS-3. However, it does not mean that there will be no humans on board MASS-3. Instead, although the ship will be controlled and operated from the control centre, there will likely be seafarers on board to deal with some work requiring technical knowledge and expertise, such as computer engineers, software developers and technicians, not to mention the completely new jobs that need to be performed on board.

MASS-4 (Degree Four): Fully autonomous ship. MASS-4 is an autonomous ship type equipped with advanced systems and devices. The responsibility for navigating and managing the ship is independent of the seafarers on board and the personnel at the control centre. The advanced decision support systems on the ship, namely *the ship control system*, make decisions and determine actions independently. Remarkably, the ship control system may have different features depending on the learning algorithms used within AI technology. Based on the learning algorithms used, it is possible to encounter two different ship control systems in terms of their technical capabilities[5]. In the first model of MASS-4, the ship control system used the classical AI algorithms has a limited ability to act within the rules determined by the programmer in decision making (MASS-4 (1)). In this case, the control system cannot go beyond the determined rules or change the result obtained. In the second model of MASS-4, the programmer could use machine learning algorithms (and deep learning); thus, learning algorithms allow the ship control system to learn from its own experience instead of setting clear rules (MASS-4 (2)).

b. Some of the Pioneering Initiatives

There are numerous autonomous shipping projects currently being carried out. While some projects are focused solely on building the autonomous ship or its technology, others examine the subject's economic and legal aspects. Yara Birkeland, for instance, is a ground-breaking project representing the future of autonomous container shipping. It has become the world's first fully electric and autonomous container ship with a cargo capacity of 120 TEU upon delivery in November 2020[6]. It completed its maiden voyage in Oslo fjord on 18 November 2021 and was put into commercial operation in Porsgrunn in early 2022. Falco is the world's first fully autonomous ferry, developed as part of the research project called 'Safer Vessel with Autonomous Navigation' (SVAN). Using the Rolls-Royce Ship Intelligence technologies, Falco completed its voyage autonomously from Parainen to Nauvo in early December 2018. Another noteworthy project is

[4] IMO, Takes First Steps.

[5] For further information *see* YILMAZ, Mustafa: Otonom Gemilerin Hukuki Boyutu, Ankara 2022, pp. 56-58.

[6] SAFETY4SEA: "Yara Birkeland delivered to its owners", 30 November 2020, <*https://safety4sea.com/yara- birkeland-delivered-to-its-owners/*> (accessed, on June 15, 2023).

Mayflower Autonomous Ship (MAS400), a fifteen-metre-long, nine-tonne fully autonomous trimaran equipped with six AI-powered cameras and thirty onboard sensors powered by solar and wind energy. MAS400 has been developed as part of the Mayflower Autonomous Ship project led by the marine research organisation ProMare and supported by a global consortium of partners, including International Business Machines Corporation (IBM). The ship is designed to collect necessary data about the ocean to improve the understanding of critical global issues affecting the marine environment, such as climate change, microplastic pollution and marine mammal conservation[7]. On 5 June 2022, the ship successfully completed a 40-day transatlantic voyage from Plymouth, UK, to Halifax, Nova Scotia, with no human captain or onboard crew.

Several initiatives are addressing the legal aspects of autonomous shipping, such as MUNIN (Maritime Unmanned Navigation through Intelligence in Networks), AAWA (Advanced Autonomous Waterborne Applications), the Comité Maritime International (CMI) Working Group for MASS and the IMO. Providing a brief overview of some of their works would be helpful. The MUNIN published various reports discussing the technical, economic, and legal aspects of autonomous shipping[28], serving as primary sources for academic works. The project has revealed that an autonomous ship is technically feasible, considering that the necessary technology for autonomy is already accessible, including but not limited to the anti-collision, electronic positioning and satellite systems, and new sensor systems based on infrared technology[8]. Notably, the MUNIN sent a legal questionnaire to multiple national maritime administrations to gather the viewpoints of states, particularly flag states, on autonomous shipping. Even though the questionnaire was sent to a limited number of respondents and the response rate was low (2/5)[9], the key takeaway is that for flag states to adopt autonomous shipping, they will require additional data on the technical capacity and reliability of these ships[10]. AAWA disclosed that while autonomous shipping could potentially reduce or eliminate human errors, it is crucial to acknowledge new risks like cyber-attacks that may arise, and they must be addressed properly.[11] The CMI established 'International Working Group on Unmanned Ships' (IWG) in 2015, then called 'Maritime Law for MASS', to identify and address the legal issues springing from implementing autonomous ships as well as raising some international awareness.[12] Remarkably, it sent a questionnaire to the 52 National Maritime Law Associations (MLA), which are members of the CMI, in early 2017. The questionnaire was

[7] STANFORD-CLARK: "For the Decade of Ocean Science, We need More Data", IBM Newsroom, <*https://newsroom.ibm.com/For-the-Decade-of-Ocean-Science,-We-Need-More-Data*> (accessed, on June 15, 2023).

[8] *See* MUNIN: "D9.3: Quantitative Assessment", Print date: 12 October 2015, GA - No: 314286; p. 3; MUNIN: "Autonomy is within reach", MUNIN Brochure 2013, <*http://www.unmanned-ship.org/munin/wp- content/uploads/2013/01/MUNIN-Brochure.pdf*> (accessed, on June 20, 2023).

[9] The names of the countries in question were not released in the MUNIN's report, since full confidentiality was promised to the concerned people so that the responses could be obtained.

[10] MUNIN: "D9.2: Quantitative Assessment", Print date: 30 September 2015, GA-No: 314286, p. 17.

[11] JOKIOINEN, Esa: "Introduction" in *Remote and Autonomous Ships- The next steps*, Rolls-Royce plc (ed.), 3- 13, AAWA Position Paper, 2016, p. 4.

[12] CMI: "Maritime Law for MASS", <*https://comitemaritime.org/work/mass/*> (accessed, on June 20, 2023). Also see EDER, Bernard: "Unmanned Vessels: Challenges Ahead", LMCLQ, V. 25, N. 1, 2019, pp. 47-56.

mainly focused on ascertaining the members' point of view concerning whether or how national laws would accommodate autonomous shipping in the light of the various international conventions such as UNCLOS, COLREG 72, SOLAS 74 and the STCW 78[13]. The findings from the survey will be provided at a later time, as deemed suitable. Finally, the IMO has been working towards incorporating autonomous ships into its regulatory framework since 2017. It explores the benefits of autonomous ships, given the safety and security concerns, the environmental impact, the potential costs to the industry and the impact on personnel on board and ashore. The IMO has conducted a review of regulations, evaluating how existing rules might be applied to ships with different levels of automation[14.]

c. Legal Status

Is it still regarded as a ship if no or very few humans are on board? This is one of the first questions that come to mind regarding autonomous shipping. Albeit a new phenomenon, a vast amount of literature has now accumulated on whether such vessels could be considered a ship at all. It must be borne in mind that there is no consistent legal classification for ships.[15] There is no single definition for a ship because each international convention assigns a specific meaning to its legal nature that is merely applicable within the context and purpose of the legal field it relates to.[16] Ultimately, upon reviewing international conventions, it appears that there are no legal obstacles to accepting the autonomous ship as a ship since the presence of humans on board is not deemed essential to the statutory concept of a ship.

II.Control Centre

a.Definition

Autonomous shipping involves two separate components or modules: the autonomous ship and the control centre. The control centre is where all necessary data is collected so that the relevant operators can remotely control or solely monitor the autonomous ship but take control in an emergency. In MASS-3, the control centre functions as the remote control, and the operator serving here will be responsible for the navigation and management of the ship. In MASS-4, the only role of the control centre is to provide supervision and control of the ship. Here, the ship's direction will be determined solely by the ship's control system, and the operators

[13] *See* CMI: "Summary of Responses to the CMI Questionnaire", <*https://comitemaritime.org/work/mass/*> (accessed, on June 20, 2023).

[14] *See* IMO: "Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)", MSC. 1/Circ. 1638, 3 June 2021.

[15] SHAW, Richard: "What is a Ship in Maritime Law?", JIML, V. 11, N. 4, 2005, p. 247; TSIMPLIS, Michael/VEAL, Robert: "The Integration of Unmanned Ships into the Lex Maritima", LMCLQ, 2017, pp. 308- 309; DANISH MARITIME AUTHORITY: "Analysis of Regulatory Barriers to Autonomous Ships", Final Report, 2017, p. 37, <*https://www.dma.dk/Documents/Publikationer/Analysis%20of%20Regulatory%20*> (accessed, on June 25, 2023).

[16] TETLEY, William: *International Maritime and Admiralty Law*, Cowansville Québec 2002, p. 35; RODRIGUEZ DELGADO, Juan P.: "The Legal Challenges of Unmanned Ships in the Private Maritime Law: What Laws would You Change?", in *Maritime, Port and Transport Law between Legacies of the Past and Modernization*, Massimiliano MUSI (ed.), Bologna 2018, p. 498; HOOYDONK, Eric V.: "The Law of Unmanned Merchant Shipping- An Exploration", JIML, V. 20, N. 3, 2014, p. 406; TSIMPLIS, Michael/VEAL, Robert: "The Integration of Unmanned Ships into the Lex Maritima", LMCLQ, 2017, pp. 308-309; DANISH MARITIME AUTHORITY, p. 37.

are not responsible for steering the ship and will not interfere with the decisions made by the system. Lastly, these facilities can be set up on the shore, land, or a platform in the sea, as well as on any stationary or moving ship.[17]

b. Legal Status

It can be difficult, even incomprehensible, to legally define an entirely new phenomenon such as the control centre hinged on existing norms and understanding. The concept of the control centre completely alters our current understanding of shipping considering the following grounds:

(1) A large number of autonomous ships will likely be steered or supervised from a single control centre;

(2) The personnel responsible for the management or the supervision of the ship will be working in shifts, which completely contradicts the traditional understanding of ‘one ship, one master;

(3) In MASS-4, the ship’s control system can have varying features based on the learning algorithms, and this could give rise to different legal implications. Many argue that the control centre could be considered a ‘virtual bridge’ that takes on the function of the bridge on the conventional ship and replaces it[18]. However, it is improbable that this matter can be resolved or should be resolved solely based on such an initial comparison, at least if it is desired to reach a radical and categorical solution. This means that new norms and standards must be established to truly address the control centre given its peculiarities.

III. Some Benefits and Limitations of MASS for Maritime Safety and Security

Autonomous shipping has both benefits and drawbacks concerning maritime safety and security. It has the potential to improve safety and security in several ways. With advanced sensor systems and AI, these ships can detect and respond to potential hazards more quickly and efficiently than human operators. Remarkably, the advanced collision avoidance systems on ships could detect and analyse the surrounding environment, assess potential collision risks, calculate optimal routes, and make necessary route adjustments in real-time. Furthermore, autonomous shipping holds great promise in mitigating human errors that often result in

[17] SÖZER, Bülent: “Self-Steering Ships”, GSÜHFD, V. 19, N. 2, 2020, p. 1367.

[18] See generally RINGBOM, Henrik: “Regulating Autonomous Ships-Concepts, Challenges and Precedents”, Ocean Development & International Law, p. 21, <*https://www.tandfonline.com/doi/*> (accessed, on June 20, 2023); SAFARI, Fariborz/SAGE, Benedicte: “Legal and Liability Analysis for Remote Controlled Vessels”, MUNIN: G.N. 314286, 2013, p. 31; RØDSETH, Ørnulf/BURMEISTER, Christoph: “Risk Assessment for an Unmanned Merchant Ship”, TransNav, V. 9, N. 3, 357-364, 2015, p. 358; KRETSCHMANN, Lutz: “Analysing the Economic Benefit of Unmanned autonomous Ships: An exploratory cost-comparison between an autonomous and a conventional bulk carrier”, RTBM, V. 25, N. 1, 2017, p. 78ff.; QUINN, Simon/VEAL, Robert/TSIMPLIS, Michael/SERDY, Andrew/NTOVAS, Alexandros: “Liability for operations in Unmanned Maritime Vehicles with Differing Levels of Autonomy”, University of Southampton, Final Report, 2016, p. 19; RINGBOM, Henrik/VEAL, Robert: “Unmanned Ships and the International Regulatory Framework”, University of Southampton, p. 6, <*https://eprints.soton.ac.uk/430534/*> (last accessed, on June 20, 2023); TSIMPLIS/VEAL, Lex Maritima, p. 316; BAUGHEN, Simon: “Who is the master now? Regulatory and Contractual Challenges of Unmanned Vessels”, in *New Technologies, Artificial Intelligence and Shipping Law in the 21st Century*, Barış SOYER & Andrew TETTENBORN (eds.), 129-148, Abingdon 2020, p. 132; PRITCHETT, Paul: “Ghost Ships: Why the Law Should Embrace Unmanned Vessel Technology”, Tul. Mar. L. J., V. 40, N. 1, 2015, p. 209; AHVENJÄRVI, Sauli: “The Human Element and Autonomous Ships”, TransNav, V. 10, N. 3, 2016, p. 519; TIMBRELL, Will: “Can the Prospect of Unmanned Ships Stay Afloat under the Current Collision Regulations”, SSLR, V. 9, N. 1, 2019, p. 54; BAUGHEN, Simon: “Unmanned Vessels and International Conventions for the Carriage of Goods by Sea”, in *Artificial Intelligence and Autonomous Shipping: Developing the International Legal Framework*, Barış SOYER & Andrew TETTENBORN (eds.), 81-98, Oxford 2021, p. 83. Also see CMI, Summary of Responses.

devastating maritime accidents by reducing or eliminating human intervention in ship operations. By lessening the impact of human factors such as fatigue, stress, and lack of attention, some incidents can be prevented, and maritime safety could be enhanced. Be that as it may, autonomous shipping should not be perceived as a foolproof solution to achieving safety and security. Installing automatic devices and systems on ships may not necessarily reduce or eliminate errors at all. There is, in fact, a shift in reliance from the captain and crew to the individuals who create, install, test, and upkeep these systems and devices, not to mention the new human factors associated with the control centre – that is, the changing nature of the human element with the centre's personnel – as well as the unknown risks deriving from the autonomous behaviours of the ship's control system as an AI robot. Lastly, there may be a period in which conventional and autonomous ships coexist in the seas. During this transition period, it is crucial to ensure the safe integration of autonomous ships into existing maritime traffic models. This includes developing protocols and communication systems that allow autonomous and conventional ships to interact effectively while minimizing the risk of collisions or other incidents. To safely navigate this transition period, it is paramount to establish a legal framework, providing sufficient training and awareness programs for seafarers and the control centre personnel.

IV. Overcoming Regulatory Challenges

The current norms, standards, rules, and regulations for maritime law and the law of the sea were not developed with MASS in mind. This work generally suggests that the challenges facing autonomous shipping can only be fully and definitively addressed through comprehensive evaluations and broad interpretations within the scope of existing conventions. Be that as it may, some key international maritime law and the law of the sea conventions, such as the UNCLOS, International Convention for the Safety of Life at Sea, 1974 (SOLAS), and Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs), will be succinctly reviewed to disclose to what extent these conventions could accommodate autonomous shipping. In the interest of brevity, this review will only touch on a few problematic provisions of these conventions in terms of autonomous shipping. For the same reason, only the findings will be submitted without delving into lengthy scholarly debates[19].

a. United Nations Convention on the Law of the Sea, 1982 (UNCLOS)

UNCLOS is the most comprehensive regulation in which the customary international law existing at the time of its adoption was compiled in many respects, and a number of innovations were introduced so as to uniformise the rules of international law for the use of seas and oceans. It is also described as the constitution for the oceans. This Convention is an essential reference point in determining the rights and obligations of States. Several Articles of UNCLOS pose obstacles to the operation of MASS. To begin with, Article 91 (1) of the Convention states that "*... there must exist a genuine link between the State and the ship...*". Given the peculiarities of autonomous shipping, especially considering there are two distinct components - the control

[19] For a more thorough discussion of autonomous shipping under international conventions and the relevant literature, please see YILMAZ, pp. 253-324.

centre and the ship- which may fall under the jurisdiction of different states, can MASS fulfil this requirement? The aforementioned term ‘genuine link’ is neither defined in UNCLOS nor the elements that constitute this link. The ambiguous wording of this provision has led many flag states to interpret it in their own economic interests. ‘The United Nations Convention on Conditions for Registration of Ships 1986’, on the other hand, where it is regulated that a genuine link can only be established if the flag state has robust control and judicial power over the ship (Article 10), did never become effective owing to the states’ lack of enthusiasm towards it. Considering the general practice of the flag of convenience, it is even debatable whether there is a genuine link between conventional ships and flag states at all. Regardless, it is submitted that Article 91 (1) of UNCLOS does not constitute an obstacle to MASS per se, as there is no direct correlation between the presence of seafarers on board and the establishment of the genuine link. Noting that the control centre may lay the foundation of new alternatives for a genuine link to be ‘truly’ established between the flag state and the ship. It would be valid if the ship’s place of nationality and the control centre’s location are under the same country’s jurisdiction. The reason is that, as noted earlier, a Turkish autonomous ship can be managed or monitored from a control centre in New York, for instance. In this case, the control centre will not be of any importance in establishing the genuine link between the ship and the flag state or in the existence of such a link.

Under Article 94 (1) of UNCLOS, states are required to effectively exercise their jurisdictions and controls in administrative, technical, and social matters pertaining to ships of their nationality. The elements constituting this critical obligation are laid down in paragraphs (2) to (7) of 94. Pursuant to Article 94 (2) (a), each State is obliged to keep a ship register containing the names and general characteristics of the ships of its nationality, with the exception of small vessels not provided for in generally accepted international regulations. The States’ exercise of their powers in administrative, technical, and social matters, in accordance with their internal laws, with regard to ships flying their flag and the crew of these ships, is set out in Article 94 (2) (b). However, in the relevant provision, the flag state is not granted the right and authority to conduct an inspection conforming to its own domestic law regarding whether the ship is equipped with seafarers. Article 94 (3) regulates the measures to be taken by the flag states so as to ensure safety at sea, posing a significant challenge to autonomous shipping. Accordingly, flag states must take particular measures for their ships, which include but are not limited to (a) the construction, equipment and seaworthiness of ships; (b) the manning of ships, labour conditions and the training of crews taking into account the applicable international instruments; (c) the use of signals, the maintenance of communications and the prevention of collisions. To further that, Article 94 (4) (b) states that a flag state must ensure that its ship has a competent and sufficient number of crew and officers responsible, especially for manoeuvring, navigating, communicating, and operating machinery, and a competent master, as required by the ship’s type, size, machinery, and equipment.

The question is: How should the words ‘master, officers and crew’ in Article 94 (4) (b) be interpreted in autonomous shipping? First, the accepted definition of captain does not require their physical presence on the ship. This does, nonetheless, not mean that the traditional definition of master will remain effective. Especially when it comes to MASS-4, there are different persons who are responsible for programming the ship before the voyage or supervising it during the entire journey. At this point, although it is open to debate which real person would be envisaged as the captain, it is more appropriate to perceive the person who monitors the ship during the entire voyage, namely the operator in the control centre, as the captain for the purpose of this provision. On the other hand, if the actual operator here, the AI robot - the ship's control system - acquires legal personhood, it will become imperative to discuss the captain's qualification for this system. During a single voyage, the control centre may change for MASS-3 and MASS-4. Furthermore, it may be necessary to have multiple operators controlling or supervising the same ship during a 24- hour period. Having multiple control centres and masters for one ship goes against the conventional understanding of 'one ship, one master'. Therefore, it is indispensable to review and update the existing definitions of 'master' at national and international levels and establish new standards for the operators. Regarding the concept of the traditional crew, it should be kept in mind that the number of crew members on board has significantly decreased over time due to technological advancements. The wording of *'... the crew is appropriate in qualification, and numbers for the type, size, machinery and equipment of the ship*' in Article 94 (4) (b) is a goal- based statement, and the number accordingly is to be determined based on the technical capacity of the ship. Meaning that it is not unfathomable to indicate that this number could even drop to zero, provided that the technology ensures the safe navigation of the ship with no or reduced humans on board. Besides, the concept of the crew in UNCLOS does not only refer to persons serving on board but also includes persons performing ship-related services outside the ship. This requirement, therefore, could be said to be met by the control centre personnel. But then again, this sort of teleological interpretation does not negate the need for establishing new norms and standards as such. Noting, however, that one of the major obstacles with UNCLOS is that its provisions cannot be easily amended, unlike other conventions for maritime law and the law of the sea. Here, as this Convention sets out general and abstract rules, the IMO and flag states may step in and fill the gaps to accommodate autonomous shipping.

Pursuant to Article 98 (1) of UNCLOS, the master of each ship is obliged to provide assistance to every person who is found at sea in danger and to whom he is informed of the need for assistance and to the ship concerned, its crew and passengers following a collision. The obligation to assist at sea is one of the oldest and most fundamental principles of international law. Seafarers accepted assisting those in distress at sea as a moral obligation long before it became a legal duty. The duty to render assistance is in question even where legal obligations in international law are not applicable. Nevertheless, as per the said provision, the duty to assist persons in danger at sea is under the sole authority and responsibility of the captain. The flag state's responsibility is to ensure that appropriate measures are taken in this regard. The captain's aforementioned duty is not without limits. It only applies provided it does not pose a severe danger to its ship, crew, and passengers. Additionally, this duty has limitations depending on the size and capacity of the ship and whether it is reasonably expected for the ship's captain to fulfil it. Above all, autonomous ships may be contrary to the spirit of Article 98 (1) of UNCLOS owing to their technical design, as these ships typically are not designed to accommodate humans. In short, fulfilling the duty of assistance outlined in Article 98 (1) of UNCLOS may not be feasible without crew on board and human spaces on ships. However, the GPS signal of such vessels can serve as a useful navigational aid for rescue, and the operators at the control centre will be able to inform the relevant rescue authorities of the position and condition of persons in distress at sea.

In accordance with Articles 22, 25 (2), 211 (3) of UNCLOS, in some instances, coastal states may impose measures that ships must comply with in their ports and inland waters. For foreign ships, they have the right and authority to make special arrangements regarding port calls. These provisions could impede the implementation of autonomous shipping. Coastal states may not permit autonomous ships to access their ports and inland waters, or they may exercise extra caution towards these ships, especially on the grounds of safety and security concerns. That is, although the good faith principle set out in Article 300 of UNCLOS requires coastal states to use their rights, jurisdiction, and freedoms responsibly, there are concerns that coastal states may misuse some of the rights and powers granted in the Convention against autonomous shipping.

b. International Convention for the Safety of Life at Sea, 1974 (SOLAS)

SOLAS 74 sets minimum safety standards for commercial ships in terms of construction, design, and equipment to ensure the safety of life at sea. Especially Chapter V, titled ‘Safety of Navigation’ of the Convention, appears to present challenges for autonomous shipping, as other chapters are related to technical rules established to ensure the safety of merchant ships. The regulations to be mainly examined in Chapter V are 14, 15 and 24.

According to the first paragraph of Regulation 14 titled ‘Ship’s Manning’, the contracting governments are under the obligation to take the necessary measures to ensure that ships flying their own flags are sufficiently and efficiently manned. It does not, however, regulate a minimum criterion regarding the numerical competence of the seafarer on board. On the other hand, it can be argued that SOLAS 74 was designed with the human element on board in mind, and therefore, the rule implicitly prohibits the absence of seafarers.

Regulation 15 includes a set of principles regarding bridge design, design and arrangement of navigational systems and equipment and bridge procedures. Currently, autonomous ships are built without a ship bridge, which is part of the cost-saving measures of autonomous shipping, enabling the ships to carry more cargo. The issue with Regulation 15 for autonomous shipping primarily concerns the technical aspect rather than the legal aspect, and it will be ineffective or meaningless for MASS without the bridge.

Regulation 24 lays down the use of heading and/or track control systems. Pursuant to the first paragraph of the Regulation, ‘*in areas of high traffic density, in conditions of restricted visibility and in all other hazardous navigational situations where heading and track control systems are in use, it shall be possible to establish manual control of the ship's steering immediately*’. The second paragraph further states that the navigational watch officers must have access to a skilled helmsperson who is always prepared to take control of steering without delay. The transition from automatic to manual steering, and vice versa, should be done by or under the supervision of a responsible officer, which is regulated in the third paragraph. As far as autonomous shipping is concerned, if the presence of human intervention is accepted as an essential element here, it can be inferred, upon first impression that this Regulation will become inapplicable to MASS. However, the relevant Regulation could be broadly interpreted, and it may be applicable depending on the ship's autonomy level. That is, for MASS-3, the task can be fulfilled by personnel in the control centre. On the other hand, if human intervention is not a determining criterion here, Regulation 24 would not hinder autonomous shipping as long as the ship's navigation is conducted safely and proficiently, even in the particular and hazardous conditions outlined.

c. Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREG 72)

COLREG 72 aims to minimise maritime accidents caused by collision, regulating the responsibility of seafarers who are expected to fulfil their duty of care properly by introducing certain standards to ensure the good management of ships. The Convention standardises the equipment that should be on board and establishes common navigational behaviour patterns to make the navigation of ships safer. The below concentrates on the primary issue in autonomous shipping within COLREG 72, which is the good seamanship principle regulated under Rule 2 (Liability), even though there may be several other rules, such as Rule 5 (Lookout) and Rule 18 (Responsibilities Between Boats), that could potentially pose obstacles.

Rule 2 (a) of COLREG 72 sets forth that '*nothing in these Rules shall exonerate any vessel, or the owner, master or crew thereof, from the consequences of any neglect to comply with these Rules or of the neglect of any precaution which may be required by the ordinary practice of seamen, or by the special circumstances of the case*'. Based on the wording of Rule 2, the duty of care or the principle of 'good seamanship' is an ultimate responsibility on the part of the ship, owner, and seafarers, and merely adhering to COLREG 72 is insufficient to discharge the obligation of exercising due diligence. In the case of autonomous shipping, who should be responsible for the reasonable care obligation as it cannot be solely attributed to the ship or its owner? First, regardless of whether the control centre personnel are considered seafarers, they will be expected to have the necessary training and qualifications to meet the duty of care. One may argue that these persons could be the ones to be expected to exercise due diligence in preventing collision at sea, especially in MASS-3. However, if, for instance, communication between the ship and the control centre is disrupted owing to data delay or loss, how can they fulfil this duty? The duty of care is principally related to human judgment, which is based partly on emotional input and partly on one's own interpretations to the extent required by the circumstances. Therefore, there is some uncertainty in regard to the effectiveness of the control centre operators who may be located thousands of miles away from the ship in terms of their awareness of the ship's conditions and ability to take appropriate precautions. Predicting the effectiveness and efficiency of remote control can be challenging. It primarily relies on the level of technology available to offer situational awareness in the control centre. On the other hand, it is apparent that the operator in the control centre would be deprived of simple inputs, such as the feeling of the seafarer while the ship is in motion, which will negatively impact resolving issues that require situational awareness.

In the survey conducted by the CMI,[20] member state organisations were asked whether the absence of seafarers on board in MASS-3 constitutes a violation of the duty of care or the principle of 'good seamanship' per se. Accordingly, eleven-member country organisations have stated that such ship operations should not be seen as contrary to the 'good seamanship' standard, solely due to the absence of seafarers on board. Three organisations argued that such ships constitute a violation of the aforementioned principle. However, eight organisations expressing a favourable opinion emphasised the necessity of ensuring the performance of operations as reliable with MASS-3 as on a conventional ship that is managed by competent seafarers. Two organisations pointed out that the principle of 'good seamanship' is a clear norm and that this principle relates to the management of the ship rather than mandating the presence of a seafarer on board. The Danish and French Maritime Law Associations, on the other hand, argued that the criteria under Rule 2 were not about where the ship was steered from but by whom it was steered, and therefore it was possible that the relevant obligation could be fulfilled by a qualified operator at the control centre.

Considering that there is human intervention in taking the necessary precautions and measures in the presence of risks that may cause a collision at sea in MASS-3, it is submitted that Rule 2 does not constitute an obstacle for MASS-3. Moreover, there is no explicit provision in Rule 2 stipulating that the intervention mentioned must be carried out by a person present on board. As a result, as per this provision, the location of the intervention, whether it be on or off the ship, is of no consequence.

Rule 2 (b) emphasizes the importance of 'good seamanship' and the duty of care. It states that '*in construing and complying with these Rules due regard shall be had to all dangers of navigation and collision and to any special circumstances, including the limitations of the vessels involved, which may make a departure from these Rules necessary to avoid immediate danger*'. Meaning that COLREG 72 does not provide a predetermined legal basis for any defense that interested parties may bring before the court regarding a collision that could have been avoided by due diligence. Before assessing MASS-4 under Rule (2), a few key points are worth noting. Artificial intelligence systems can adapt to the social environment in which they are found by following a similar learning method to humans. They can learn from mistakes and accidents. If the relevant rule does not require human intervention and the ship control system, which is an AI robot, can provide the same level of care and attention as the captain and crew, then one may argue that it can fulfil this duty. Be that as it may, adhering to or imposing a notion that has been purely established for conventional shipping, like the good seamanship principle, would be no longer efficacious in MASS-4 in particular and in autonomous shipping in general.

d. Maritime Autonomous Surface Ships Code (MASS Code)

As technology advances, it brings both opportunities and challenges. The IMO's goal is to carefully consider the benefits and drawbacks of these developments to create new norms suitable for emerging technologies. To that end, since 2017, under the coordination of the IMO Maritime Safety Committee (MSC),

[20] See CMI, Summary of Responses.

several sessions have been held to discuss the compatibility of various applicable regulations with autonomous shipping, including SOLAS 74, COLREG 72, STCW 78, STCW-F 1995, LL 1966 (loading and stability regulations), SAR 1979 (search and rescue regulations), Tonnage Convention 1969 (tonnage measurement regulations) and STP 1971 and SPACE STP (regulations on private commercial passenger ships). During the MSC sessions, regulatory scoping studies focused primarily on autonomous ships and identified necessary revisions for their operations. The study of MSC has placed significant importance on understanding the terminology and varying levels of autonomy. In addition, the MSC has analysed the definitions of ‘captain’ and ‘crew’ in various conventions. The findings indicate that the interpretation assigned to these terms in several international conventions lacks clarity, and the scope of their duties and obligations is not well-defined.

In the MSC sessions, the seafaring qualification of the personnel serving at the control centre was identified as a potential gap. It was highlighted that the control centre is an utterly new phenomenon, and it is essential to provide an explanation of its operation and functions. During the MSC sessions, the discussions focused on the challenging clauses of the conventions for autonomous shipping mentioned earlier. It has been noted that the main concerns regarding autonomous shipping are centred around three key areas: the autonomous ship itself, the control centre, and the legal status of its personnel, and argued that it would be more appropriate to conduct regulatory studies based on these common potential gaps or themes.

To address these issues effectively, creating a distinct ‘MASS Code’ specifically for autonomous shipping is optimal. This idea was discussed for the first time in detail at the 103rd session of the MSC, held between 5-14 May 2021, and it was decided to create an independent Code, considering the different types of autonomous ships. The MASS Code will consist of the amendments made in the SOLAS 74 and STCW 78 Convention and other IMO conventions deemed necessary to be implemented, thus filling the legal gap. Of course, interim guidelines to be published by the IMO for autonomous ships will be of great importance to provide safe, secure, and environmentally friendly autonomous ship operations and lay the groundwork for the implementation of the MASS Code. At the MSC session held from 20-29 April 2022, it was stated that a non-mandatory MASS Code would be adopted in the second half of 2024, while the effective date of the mandatory Code is to be 1 January 2028.

V.Conclusion

Autonomous shipping has advantages in terms of safety and security, but it also poses risks and dangers. These include concerns around human factors, collision avoidance, technical failures, cybersecurity threats, reliability of remote control, and environmental protection. The problems at hand cannot be solved by relying solely on existing norms, standards, rules, and regulations, as they are insufficient to address them adequately. Even though it is vital to explore if existing national and international laws hinder such ship operations, the key issue should not be the compliance of these ships with the conventions or how to make them comply, but rather the need to establish appropriate rules that meet the requirements of these ships. The notion that the extant regulations can be broadly interpreted to accommodate autonomous shipping is, therefore, unreasonable and does not offer radical and categorical solutions. In short, modern methods and approaches should be developed and employed in a way that properly identifies and addresses the challenges posed by autonomous shipping.

USAGE OF MARITIME UNMANNED SYSTEMS IN SUPPORT OF MSO

Cdr. (PRT N) Francisco CAVACO –

The presentation titled “Usage of Maritime Unmanned Systems in Support of Maritime Security Operations” was delivered by CDR Francisco Cavaco, the Maritime Situational Awareness staff officer at MARSEC COE. The presentation focused on the concept development efforts on the usage of Maritime Unmanned Systems (MUS) in Maritime Security Operations (MSO).

The presentation began with an introduction to the focus areas of MARSEC COE and the definitions of maritime security and maritime security operations. It emphasized the importance of adhering to international and national laws, preserving the right of navigation, and ensuring the safety of citizens, vessels, infrastructure, and resources.

The presentation then moved on to discuss the mission and vision of MARSEC COE, highlighting seven key tasks: Protection of Critical Infrastructure, Supporting Maritime Counter Terrorism, Fighting Against Proliferation of Weapons of Mass Destruction, Contributing to Maritime Security Capacity Building, Supporting Maritime Situational Awareness (MSA), Upholding Freedom Of Navigation, and Maritime Interdiction Operations.

The speaker provided insights into how unmanned systems can be linked with MSO tasks. He mentioned that Allied Maritime Command (MARCOM) requested MARSEC COE to develop a concept for maritime unmanned systems employment in support of maritime security operations. The concept focuses on how MUS can be employed in MSO, considering experiences from past and current NATO maritime security operations.

Unmanned systems have been used as platforms for intelligence collection, surveillance, and reconnaissance (ISR), enhancing MSA by providing more accurate and sustainable data. The adaptability, versatility, and cost-effectiveness of unmanned systems have been indispensable to successful maritime operations.

The speaker discussed the drafted vision of the Concept of Usage of UAS and MUS ISO MSO. He highlighted several fundamental MUS employment principles addressed in the drafted concept, including interoperability, legality, safety, manned-unmanned teaming, adaptability, and effectiveness.

The second part of the presentation, continued with the discussion on the audience's willingness and eagerness to both use and fight against Maritime Unmanned Systems (MUS). The speaker noted that the audience recognized the threat posed by low-observable MUS in the hands of ill-intended actors as having tactical game-changing potential.

The speaker highlighted that responding to threats posed by unfriendly usage of MUS involved tightening EMCON policy and adapting force posture. He emphasized that MUS threats considerably complicate the maritime landscape and adversely affect the goal of a well-rounded and established Maritime Situational Awareness (MSA) in the operational space.

The speaker then discussed the need for guidance in MUS development, given the heavy interest of the private sector. He suggested that guidelines and requirements should be summed up to a broader development framework, so that requirement and development do not end up chasing one another in a contingent or hazarded way.

The speaker shared that MARSEC COE has conducted three workshops and participated in the Uncrewed Maritime Systems Technology (UMST) conference 2023, which have been valuable in informing their concept. He noted that all countries agree on using MUS for Maritime Situational Awareness (MSA) purposes, but legal aspects of MUS Usage for MSO must be critically considered.

The speaker also discussed the legal status determination of MUS and its direct consequence on their entitlement to perform certain important maritime security operations functions. He mentioned the United Nations Convention on the Law of the Sea (UNCLOS) and its regulations on activities only for peaceful purposes. He emphasized that the use of coercive force during law enforcement operations is strictly limited to the presence of law enforcement officials on board of the intervening vessels.

The final part of the presentation on “Usage of Maritime Unmanned Systems in Support of Maritime Security Operations” delved into more specific examples and challenges related to the use of Maritime Unmanned Systems (MUS).

The speaker raised several thought-provoking questions about the legal implications of MUS usage, such as whether a warship can pursue an unmanned system, or whether an unmanned system can visit a ship or another unmanned system.

The speaker then discussed various aspects of MUS usage, including the integration of AI into all MUS, the challenges of integrating with command and control systems, the need for policy, doctrine, and concept development beyond the tactical level, and the environmental limitations of MUS. He also highlighted the need for decision support tools for data fusion and compilation, and noted that launching and recovering MUS remains a difficulty.

Regarding Maritime Security Operations (MSO), the speaker pointed out that MUS extend the sensor range of the vessels from which they were deployed, enable development of recognized maritime picture and pattern of life, enable interdiction operations, and can intervene in critical subsea infrastructure. However, he also noted that MUS require better beyond line of sight communications capabilities and there is limited physical interoperability between organic or shore-based MUS.

The speaker concluded by mentioning upcoming events such as EXER MARSEC-23 Final Coordination Conference Operational Experimentation (OPEX) Planning Syndicate, DYMS23 in September 2023, EXER MARSEC-23 OPEX on 09-20 October 2023, and the Usage of MUS in MSO Concept Development Workshop on 30 November 2023.

This comprehensive presentation provided valuable insights into the usage of Maritime Unmanned Systems in support of Maritime Security Operations.

USAGE OF MARITIME UNMANNED SYSTEMS IN MSO – OPEX

Cdr. (TUR N) Hatice GÖMENGİL –

The presentation titled “Operational Experimentation (OPEX) in October 2023” was delivered by Cdr. Hatice GÖMENGİL. The presentation focused on the execution of the OPEX, which is a key element of the concept development process for the usage of Maritime Unmanned Systems (MUS) in Maritime Security Operations (MSO).

The speaker emphasized the importance of collaboration and collective input in developing a comprehensive concept and a successful OPEX. The speaker also highlighted the importance of the participants’ experience and insights in this process.

The presentation covered a range of topics related to the OPEX, including the integration of AI into all MUS, the challenges of integrating with command and control systems, and the need for policy, doctrine, and concept development beyond the tactical level.

The speaker also discussed the legal implications of MUS usage, such as whether a warship can pursue an unmanned system, or whether an unmanned system can visit a ship or another unmanned system.

The speaker concluded by discussing upcoming events such as EXER MARSEC-23 Final Coordination Conference Operational Experimentation (OPEX) Planning Syndicate, DYMS23 in September 2023, EXER MARSEC-23 OPEX on 09-20 October 2023, and the Usage of MUS in MSO Concept Development Workshop on 30 November 2023.

This comprehensive presentation provided valuable insights into the usage of Maritime Unmanned Systems in support of Maritime Security Operations.

EFFECTIVENESS ANALYSIS OF UNMANNED SURFACE VEHICLES IN LITTORAL WATERS

Mr. Mehmet Akif ÇEVİK:

The presentation titled “Effectiveness Analysis of Unmanned Surface Vehicles in Littoral Waters” was delivered by a former member of MARSEC COE. The presentation began with an overview of Unmanned Surface Vehicles (USVs), highlighting the ongoing process of standardizing USV usage and the need for more data collection to implement a safe way of autonomy.

The speaker briefly summarized the legal background of USV usage, emphasizing the need for elements of trust, situational awareness, a robust framework for navigation and communication, and safety standards.

The presentation then delved into naval warfare in littoral waters, highlighting its conceptual similarity to naval warfare in open sea but significant differences in details. The speaker emphasized the importance of clear concepts, doctrines, plans, high level of training for readiness, situational awareness at sea, flexible tactics for rapidly changing tactical environment, C2 capabilities using advanced technological infrastructure, and close coordination between military units.

The speaker discussed the simulation environment as a cost-effective way to test defense systems, evaluate system effectiveness, and supply synthetic data. He highlighted the potential roles of USVs in littoral naval warfare concept such as Anti-Surface Warfare (ASuW), Anti Air Warfare (AAW), Anti-Submarine Warfare (ASW), Mine Warfare (MW), Intelligence, Surveillance, Reconnaissance (ISR), Electronic Warfare (EW), and Goalkeeper role for HVUs.

The speaker concluded by stating that USV technologies are rapidly developing but need a solid framework. He suggested that civilian applications in high-seas could precede military applications due to military design complexity. He also emphasized that while USVs have not been in real scenarios like UAVs, they will play a crucial role in future maritime operations.

NATO DEFENSE PLANS AND THE MARITIME DOMAIN

Mr. Ferhat Arda KARAKAYA
NATO IS Head of Plans

I'd like to share some insights, but discussing detailed plans in a non-classified environment can be challenging. The most intriguing aspects of the plans, such as the scenario and commandments, are often classified. However, I'll attempt to explain the implications of NATO's new planning structure in this setting. One key takeaway from this meeting is understanding the new planning structure of NATO. The second point is more of a rhetorical question, but it's crucial in the maritime domain. The strategic concept related to maritime security has been quoted by the director. I'd like to add a powerful sentence from it: "The Euro Atlantic area is not at peace." This statement is a fact, given the ongoing conflict in Ukraine, and it has serious implications for how we think about deterrence plans in the maritime domain. We've been accustomed to viewing peace, crisis, and conflict in a linear fashion, a mindset that was ingrained in us during the post-cold war era when we were primarily dealing with out-of-area operations. During that time, NATO had the luxury of controlling time and space. However, the current situation requires a different approach.

The maritime domain is a key area for the Alliance, but we need to rethink our approach to it. Our current maritime posture has three functions: security, strategic and warfighting. These were designed for a peaceful Euro Atlantic area, but now we face new challenges and threats. We need to adapt our posture to the changing environment and be ready for any scenario. One way to do this is to develop regional plans that are aligned with the Alliance's strategic concept. These plans will guide our actions and responses in different regions and situations. We have already activated some of these plans after the Russian invasion, and they have helped us prevent the conflict from escalating. However, we still have a lot of work to do to improve our maritime capabilities and cooperation. This is the main message I want to convey to you today.

In the past, NATO's military strategy was defined by its Strategic Concept, a practice that was prevalent during the Cold War. However, the 2010 Strategic Concept did not facilitate the development of a new military strategy. As a result, the process was somewhat reversed. The military strategy and the DPA, both classified documents, were developed first, and their themes were then incorporated into the Strategic Concept, which is the focus of our discussion. This approach has allowed for the refinement of many themes found in these documents.

Regarding the maritime domain, NATO's plans can be visualized as a pyramid. At the top, there's a strategic level plan, followed by domain and function-specific plans. At the base, there are regional plans that resemble traditional military plans, focusing on specific geographies, adversaries, and command arrangements. The goal is to integrate all these elements by the upcoming summit.

The defense ministers of NATO will meet in Brussels tomorrow and Friday, but the key decisions will likely be made by the heads of state and government at the summit in about a month. These decisions will be communicated to the public through the summit communique.

Shifting from a broader perspective to the maritime sector, it's important to note that the area of responsibility encompasses 82% of water, a figure that has recently increased with the accession of Finland. The seas are continuous and interconnected with other domains and areas. The strength of our strategic approach to DDA comes from recognizing these connections and incorporating them into a single strategic framework, something that was lacking in the post-Cold War period.

On any given day, national activities make up 80-90% of the operations, but these are increasingly coordinated by NATO. This is particularly true in the maritime domain, although the air domain also plays a significant role. For instance, the recent NATO exercise in Germany, the largest air exercise of the post-Cold War era, involved 250 aircraft from 24 allies and one partner. This exercise gave us a glimpse of what a collective defense scenario would look like and emphasized the need for a whole-of-government approach to collective defense across land, sea, and air.

Lastly, the importance of a federated or synchronized approach extends beyond just the allies and NATO, but also between civilian and military sectors. For example, at a conference in Copenhagen focused on Baltic security, the idea of equipping civilian fishing ships with sensors to maintain maritime situational awareness was discussed. While no decision has been made, it highlights the complexities and considerations involved in modernizing our collective defense system.

THE INDO-PACIFIC SECURITY IMPORTANCE FOR THE ALLIANCE – NATO STRATEGIC CONCEPT AND NATO STRATEGIC FORESIGHT PERSPECTIVES REPORT

Dr. Joanna Siekiera

Fellow at the Brute Krulak Center for Innovation & Future Warfare, US Marine Corps University.
External Consultant and Editor at the NATO Stability Policing Centre of Excellence in Vicenza, Italy

I. Introduction

The Indian Ocean and the Pacific Ocean lay on the other side of the globe from the perspective of Europe, where the vast majority of the North Atlantic Treaty Organization's (NATO) members are. Thus, from this European (or Eurocentric) perspective the Indo-Pacific region remains somehow neglected in geostrategic analysis, academic debate, and military training. This situation, however, is getting improved. The impact of regional affairs, both political, economic, and security ones, on one continent highly impacts other continents. Indeed, the Indo- Pacific mechanisms, dilemmas, and challenges impose vital consideration on the Euro-Atlantic community, too.

This article is therefore an attempt to present the relevance of the Indo-Pacific region for NATO, as well as to argue that our, Euro-Atlantic, security is intertwined with the good functioning defense alliances and mechanisms across the Indian and Pacific Oceans. Such analysis will be done from the international law standpoint, as such a legal view is still very often missed in military considerations on regional and global security, thus requiring more attention in order to fully comprehend the broad picture and foresee future scenarios. The two documents will be used to analyze the topic, namely the 2022 NATO Strategic Concept and the 2022 NATO Strategic Foresight Analysis: Regional Perspectives Report on the Indo-Pacific (herein as the NATO Report). The first text can be seen, despite its political while not legal validity, as *lex generalis*. It reaffirms the Alliance's three core tasks: deterrence and defense, crisis prevention and management, and cooperative security. The Indo-Pacific, geographically outside of the scope of this intergovernmental organization's functioning, has been placed among areas of strategic importance for NATO, unlike ever before.

The NATO Report brings a strategic analysis at critical times when undeniably the discussed region becomes increasingly important for both the security and defense policy of Allies and its Partners. Here, already at the beginning of this article, those partners must be recalled. Australia, New Zealand, Japan, and the Republic of Korea, being not only non-members of the Organizations nor its associates as the North Atlantic Treaty[21] does not provide for such a category, but also lie outside of the territorial scope were invited for the NATO Summit in 2022. This unprecedented participation in the Alliance's highest meetings of the

[21] The North Atlantic Treaty, also called the Washington Treaty, establishing NATO was signed on April 4th, 1949.

heads of state and government clearly showed how much NATO values and, pragmatically speaking, needs those like-minded states from the Indo-Pacific region.

II. Indo-Pacific – a new center of gravity

NATO has increased its awareness of the Indo-Pacific along with all the political, economic, and security challenges of the region. The changes happening in our eyes, human, technological, and environmental themes in Asia and Oceania have and will continue to shape the global future affecting the Euro-Atlantic area with an intensified effect. The preparedness for such must be aligned with understanding the unique, so much different from our Western civilizational mindset, dynamics of values, including legal values and legal culture. But what is legal culture? It can be understood as the entirety of habits and values related to the acceptance, assessment, criticism, and finally also implementation of the law in force, thus also the actual readiness to comply with the norms of such law. Consequently, for Western democracies legal culture is the political and societal system guaranteeing the protection of values and legal goods that are important for society, which such a society protects through its institutional and administrative framework. Also, in this way, citizens legitimize their authorities, who are, after all, the guarantors of social order ensuring development and security – both national, and external, military, energy, and recently also climate security (Siekiera 2022).

The rise of China, having consequences far beyond the Indo-Pacific region, does challenge the Alliance's interests, values, and security. Chinese aggressive politics regionally and globally must be named and stopped, while its devastating effects on local economies, legal-political systems, and defense capacity must be reversed. The People's Republic of China's (PRC) ambitions towards Asia and Oceania are successful by virtue of the sea-level rise in those poor, undeveloped, and unstable states. But sea-level rise, with all its biological-chemical-physical consequences, poses huge legal threats to the stability of the whole region, where shrinking islets and larger territories become inhabitable, is causing a myriad of legal dilemmas. Those legal questions concern the most fundamental aspects of a state's sovereignty, territorial integrity, economic rights, and security matters. Lastly, the seabed is hiding the most precious raw materials, which can be used for or against us and the international law-based order. Yet, if technology, developing at a dizzying pace, will not be aligned with the law (new and adapted to modern conditions), we might not be able to prevent the most damaging war for humanity – the war for resources.

a. China in Great Power Competition

The values presented by the PRC are not only incompatible with human rights, human dignity, and the democratic system, but they have already legitimized illegal and inhuman acts of murder, abduction, detention, torture, sterilizing, and forced abortions on their own citizens, political opponents, religious, ethnical, national, and sexual minorities. Economic and technological espionage, widespread corruption at ministerial levels of developing and developed countries, in humanitarian organizations, as well as in engineering aid projects cannot be left unsaid either. The predominantly successful Chinese attempt and efforts to economically, diplomatically, culturally, and even militarily federate states in the Indo-Pacific have been putting at risk the rule of law and international order, including maritime freedom. The latter must not be omitted as that is the maritime trade which has been an essential aspect of global commerce for centuries. Now this low-cost, efficient, and peaceful method of transporting goods is under threat.

As NATO does not have its own policy for the Indo-Pacific, it appears necessary to recall here political and diplomatic interests in this region of certain Allies and our partners. Unquestionably, it is the United States' largest interest to prevent China from maintaining and/or expanding its sphere of influence over the Pacific Ocean. Moves by the PRC to claim sovereignty over disputed territories, including maritime territories, especially in the South China Sea, efforts to establish alternative international financial institutions, the open statement that since now that is China and Russia will be guarding over the world order based on international law, [thus their authoritarian interpretation]", and development of military capabilities aimed directly at the U.S. capabilities [like signing the military pact with the Solomon Island allowing the People's Liberation Army Navy the stable present in Oceania] suggest China is taking a competitive stance towards the US (McDonald 2023). "China is also the first great power since prewar Japan to challenge U.S. maritime supremacy, a post-World War II cornerstone of U.S. global power and national security. The rise of China challenges U.S. security in a region vital to security." (Ross 2018)

This geopolitical and security reasoning of what is called Great Power Competition also explains the pivot from "Asia-Pacific" to "Indo-Pacific". Hence, the terminology must have been changed in order to incorporate the external policy of Washington over Asia and Oceania. As "Asia-Pacific" refers mainly to an economic construct, which gained popularity over the 1980s during the process of regionalization as the alternative to globalization, it did not take into consideration India or the Indian Ocean. Over the course of time, though, Indian influence, as well as its growing economic power regionally and globally should not be left outside of this geopolitical equation. New Delhi is equally aware of its own regional and global influence and thus power – economic, but perhaps military, too in the foreseeable future. In the academic and political analysis, India is called "the balancer" in the Indo-Pacific (Malhotra 2023, Naidu 2001), yet we can argue that such a role will not be sufficient for the largest navy in the Indian Ocean and the fastest-growing economy in the world.

b. Sea-level rise

Climate change is perceived as one of the most challenging threats to humankind. It is also recalled in the NATO Strategic Concept: "The Alliance will lead efforts to assess the impact of climate change on defense and security and address those challenges. We will contribute to combatting climate change by reducing greenhouse gas emissions, improving energy efficiency, investing in the transition to clean energy sources, and leveraging green technologies while ensuring military effectiveness and a credible deterrence and defense posture"[22].

[22] Paragraph 46 of the 2022 NATO Strategic Concept.

The ocean plays an essential role in mitigating climate change by serving as a major heat and carbon sink. Yet, the ocean itself bears the brunt of global warming, which is evidenced by changes in the temperature of water and air, acidification, currents, the sea-level rise, affecting the health of marine species, nearshore, and deep ocean ecosystems. Other less known yet equally severe consequences of climate change to the maritime environment are seasonal shifts in species, coral bleaching, coastal inundation, coastal erosion, harmful algal blooms, hypoxic (lacking oxygen) zones, new marine diseases, loss of marine mammals, changes in levels of precipitation, and fishery declines. In addition, more extreme weather events, such as droughts, floods, and storms occur[23].

Besides the dreadful effects of climate change on the ocean, societal implications must be also pointed out. As ocean change [how the author prefers to name the climate change impact on the ocean] is increasingly altering the ocean’s chemistry, underwater cultural heritage sites are being threatened by ocean acidification. “Irreparable harm is likely, however, restoring coastal ecosystems, reducing land-based pollution, reducing CO2 emissions, reducing marine stressors, increasing historic site monitoring, and developing legal strategies can reduce the devastation of underwater cultural heritage sites”. (Spalding 2011). For Oceania inhabitants, as well as for the Indian Ocean poor, developing island states, low-lying states, coastal states, and deltaic states, the ocean is a home – it feeds them, protects them, and enables them to grow and prosper. It must be underlined that the level of poverty in that region is immense [which is clear in the statistics by the World Bank, the Association of Southeast Asian Nations (ASEAN), and various organizations, but also witnessed by the author herself who sailed across the Pacific Ocean in July-August 2022]. Small island states do not have any industry, while the main branch of national economies is fishing. In addition, (tuna) fishing provides the major, or very often only source of protein. The second branch of the economy is tourism. However, tourism requires proper and modern infrastructure, while the budgets are limited and rely on fishing and tourism. Also, during and after the COVID pandemic, visitors stopped coming causing enormous budgetary holes, but even before that, due to global warming other warm destinations, much closer to potential tourists’ homes, became popular minding lesser costs and more convenient ways to reach, instead of the far Indo-Pacific.

Without a reliable economy, good, or at least enough or sufficiently functioning, infrastructure, gigantic problems with democratic institutions [undeniably connected with the colonial period and negative perception of state institutions, what legal scholars called now “the imposed law” in the Pacific], those states become an easy target for China determined to reshape the economic and military balance of the region. Beijing’s values and priorities are pushed into the new global governance system, as well as bilateral relations build on

[23] More on this topic read „Ocean and Climate Change” by the Ocean Foundations: https://oceanfdn.org/ocean-and- climate-change/

"civilizational aid", also against climate change effects. Thus, sea-level rise became an easy, yet very effective, excuse for the PRC to interfere in internal matters [including the establishment of shadow governance structures] of the Indo-Pacific states, which are unable to fight ocean change themselves.

c. Future war for sea-bed raw materials

The seas around Pacific Island countries are at the center of interest for deep seabed mining. The industrialized world's hunger for raw materials has already its cost in Asia, Africa, and Latin America: "People living in the areas of the oil and mining ventures, already stricken by poverty, are left with polluted waters and soils, skin and respiratory conditions, the expropriation of their land without adequate compensation, expulsion, and the destruction of long-existing social structures and cultures. Old conflicts between ethnic groups, communities and families, and conflicts within them, are inflamed and new ones ignited. Those who fight with peaceful means to have their economic, social, and cultural rights respected and protected, along with the right to adequate food, clean water, health, housing, education, and decent work, are politically persecuted. They can be subject to arbitrary detention, trumped-up charges, or intimidation; in the worst case they can be threatened with death, made to 'disappear' or even extrajudicially executed" (MISEREOR 2016).

As demand grows globally for cobalt, copper, and nickel needed to make batteries for electric vehicles, one of the richest untapped sources of the raw materials lies 2½ miles beneath the surface of the Pacific Ocean, "enough to power 280 million electric vehicles" (Lipton 2022). As no mining has ever been done on a scale like this on the planet, legal questions arise. The ecological impacts of mining on deep-sea ecosystems are still inadequately evaluated. Furthermore, marine mining will undoubtedly cause conflicts with various stakeholders such as fisheries, offshore wind farms, communications cable owners, and tourism. Also, as was mentioned above, the ocean is an immense source of food, energy, clean water, and various ecosystem services and has already been suffering seriously from multiple stressors from anthropogenic sources (Sakellariadou et al. 2022).

The Seabed Authority, established under the auspices of the United Nations (UN) by the 1982 Convention on the Law of the Sea (UNCLOS) to govern seabed exploration and extraction, is in fact too weak and not equipped in either legal (enforcement) or technical tools to control seabed mining, prevent a breach of the law of the sea and lastly to punish any form of such actions to the detriment of all humankind. On the other hand, though, the mining industry claims that seabed mining would be for the benefit of humankind, as it was required under the UNCLOS causing far less ecological damage than open-pit mining. Undoubtedly, raw minerals lying in the Pacific Ocean can be used in medicine.

As every member of the UN is *ipso facto* a member of the Seabed Authority[24], every one of them can seek

[24] Art. 156 (2) of the UN Convention on the Law of the Sea.

permission to conduct surveys to identify mining sites[25]. Canada, China, France, Germany, India, and the Republic of Korea are among other richer states, that have done that. Right of access to the sea and freedom of transit, as well as freedom of the high seas, are the common heritage of humankind[26], which means those rights and freedoms belong to every state and every individual. Though *de iure* it looks obvious, yet *de facto* one can imagine only the richest, most developed nations would be able to afford seabed exploration and extraction, while negative effects of such industry will be borne by the poor, undeveloped island states in the Pacific – the surrounding maritime zones. Such an environmental situation, just like already is with sea-level rise, will be very easily used for political goals, where global players would back up their regional partners. Such a scenario might, but of course not necessarily, end up with (a) military conflict(s) for resources.

III. NATO Strategic Concept

The NATO 2022 Strategic Concept adopted at the Madrid Summit is novel due to many reasons. First of all, it presents one of the most significant policy shifts in the Alliance's deterrence policy since the end of the Cold War. The Russian Federation was categorically recognized as the most significant and direct threat to the security and stability of the Euro-Atlantic region. The People's Republic of China, in turn, was declared as a security challenge to our interests, security, and values. The mutual strategic attempts of both Russia and China to undercut the rules-based international order were also named in the Concept. Again, it is highly important from the NATO side, being a political-military organization, to call adequately the threats to its member states, but also the entire international community. Such shared awareness enhances the resilience and preparedness of the Alliance against any threats or the use of force – let it be military or economic. Maritime security was listed among other domains which were places as substantial for NATO peace and prosperity. In order to deter and defend the values, stability, and prosperity of the member states and their partners it is necessary to "uphold freedom of navigation, secure maritime trade routes and protect our main lines of communications"[27].

Freedom of navigation is one of the most fundamental principles in the law of the sea. Art. 87 of UNCLOS enlists other freedoms steaming from the freedom of the high seas, being freedom of overflight, freedom to lay submarine cables and pipelines, freedom to construct artificial islands and other installations permitted under international law, freedom of fishing, and freedom of scientific research.

According to the NATO 2022 Strategic Concept, both Russia and China are threatening this freedom. As the Russian Federation is modernizing its nuclear forces and expanding its novel and disruptive systems, employing coercive nuclear signaling, Moscow is in fact aiming to destabilize a broad range of regions in

[25] Art. 17(2)(b)(ii).

[26] Previously called "the common heritage of mankind".

[27] Paragraph 23 of the 2022 NATO Strategic Concept.

Europe and Asia. In addition, in the Arctic ("the High North" in the Concept), Russia's capability to disrupt NATO's reinforcements and freedom of navigation across the North Atlantic appears as a strategic challenge. Lastly, Moscow's military build-up in the Baltic, Black, and Mediterranean Sea regions, along with its military integration with another authoritarian regime – Belarus – challenge our security and interests.

The PRC seeks to control key technological and industrial sectors, critical infrastructure, including maritime infrastructure and transport, and strategic materials, including those at the seabed of the Pacific Ocean. The Navy People's Liberation Army Navy has been under modernization for 3 decades, which transformed it into a much more modern and capable force. China's navy is not only the largest naval force within China's near-seas region, which allows the PRC to conduct a growing number of operations in the Western Pacific, the Indian Ocean, and waters around Europe. It is estimated that sometime between 2015 and 2020 the Chinese Navy surpassed the U.S. Navy (USNI 2023).

The Indo-Pacific is mentioned only two times in the NATO 2022 Strategic Concept which is still more than ever in the history of the Alliance. The region is "important for NATO, given that developments in that region can directly affect Euro-Atlantic security. We will strengthen dialogue and cooperation with new and existing partners in the Indo-Pacific to tackle cross- regional challenges and shared security interests"[28]. The Alliance and its partners, both strategic partners from the Pacific Ocean, as well as the Indian Ocean have similar, yet slightly different perceptions of maritime security. As one can guess easily, it depends on the economic growth and the state's interests. The best example portraying this approach is the nomenclature of the freedom of navigation strategies in the Indo-Pacific region. The Japanese government opts for the Indo-Pacific being "free and open"[29], Indian – "free, open, and inclusive"[30], Australian – "open, stable, secure and prosper"[31], while American – "free and open, connected, prosperous, resilient, and secure"[32]

IV.NATO Strategic Foresight Perspectives Report

Great Power Competition (GPC) initially described geopolitical perceptions of economic- political-military rivalry between the hegemonic US and aggressive tactics by the PRC. Yet, minding all the dynamics and interdependence of political and cultural factors, including legal culture, GPC should be seen as a strategic challenge between the Western civilization nations and Chinese allies or at least like-minded authoritarian regimes, primarily Russia, Belarus, Iran, North Korea, and Syria. Here Russian resurgence, its military rebuild

[28] Paragraph 45 of the NATO Strategic Concept.

[29] Ministry of Foreign Affairs of Japan, Free and Open Indo-Pacific (24.04.2023): https://www.mofa.go.jp/policy/page25e_000278.html

[30], Outlook India, *India Commits To A Free, Open And Inclusive Indo-Pacific Region* (23.05.2023): https://www.outlookindia.com/business/india-commits-to-a-free-open-and-inclusive-indo-pacific-region-news- 198108

[31] Australian Department of Foreign Affairs and Trade, *Realising the Pacific's vision for stability, security and prosperity* (7.06.2019): https://www.dfat.gov.au/news/speeches/Pages/realising-the-pacifics-vision-for-stability- security-and-prosperity

[32] The White House, *Indo-Pacific Strategy of the United States* (11.02.2022): https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/11/fact-sheet-indo-pacific-strategy-of-the-united-states/

displayed in Syria, South Caucasus, Libya, Ukraine, and even farther in Africa, cannot be unnoticed either. Emerging and disruptive technologies (EDTs), as well as psychological operations (PSYOP) and informational warfare (IO) on social networking platforms used by undemocratic regimes contest the core principles of international security built on the international law order. In order to effectively tackle those problems, understand their true nature, alter our tools in hybrid warfare, and, if possible, prevent such irregular conflicts in advance, if not – fight them back, we must stay united within the Alliance, but also keep close our partners. Thus, in the era of GPC, NATO must work even more closely with like-minded states from Asia and Oceania. 31 member states along with Australia, New Zealand, the Republic of Korea, and Japan agreed to step up political dialogue and launch practical cooperation and coordination. Here is essential to establish legal mechanisms in case of an "emergency". Each partner state is a sovereign state and thus operates in its own separate legal system, where all those internal legal regimes of the Alliance and partners sum up to 35. Hence, political statements must be seen as a beginning, but the essential arrangements must be implemented at the national levels (Siekiera 2022b).

The Strategic Report clearly states, also in a much more direct manner than the Strategic Concept, that China and Russia offer a new regional alternative for the poor, developing states of the Indo-Pacific region, who are already struggling with a very existence. President's Xi Jinping and Vladimir Putin are attempting to challenge a free and open basis for establishing international relations. Such basis ought to be "voluntary", with the core element of the free will of nations, according to international law. The NATO Report foresees the Indo-Pacific is likely to convert into a predominant Chinese federation or potentially constrain split countries through economic, diplomatic, cultural, and military levers. Such division and heavy dependence on the PRC's system of values has already put "at risk the rule of law, international order, democratic values, maritime freedom, sovereignty, and territorial integrity[33]."

What is more, an already seen in the Indo-Pacific region shift from the rule-based order is paired by Beijing with the experience of the COVID-19 pandemic, increasing use of power politics, including military diplomacy, and the climate-related security implications for small island states in Oceania. That is why this detailed and diligent NATO document on the Indo-Pacific is so crucial to identify regional trends, which might not be easy to recognize or categorize from the European or Northern American perspective. The Strategic Report is also fundamental to provide the Alliance with possible scenarios out to 2040 and beyond. Only then, after recognizing socio-economic trends in Asia and Oceania, NATO can be ready to combine defense and security implications on a broader than just a regional scale. The last step here would be specifying the political-military means to deter and defend, in order to protect the common values of the Allies.

As the aim of this article is to present why the Indo-Pacific matters for NATO, some additional facts should

[33] Paragraph 2 of the NATO Strategic Foresight Perspectives Report.

be recalled. Demographic trends show that already now more than half of the Earth's population lives in the Info-Pacific, while China, India, Bangladesh, Pakistan, and Indonesia are the most populated countries in the world. Also, the population of this region is projected to reach 5 billion, which means an almost 12% rise[34]. Economically, the 2018 Trans- Pacific Partnership[35] and the 2022 Regional Comprehensive Economic Partnership[36] created the world's largest free trade zone. Yet, the "free trade area" does not provide many institutional or technical details, of a huge importance for national economies, thus these arrangements are seen by both the US and India as merely geopolitical interference and "Chinese statecraft in the region"[37]. In other words, in the next 2 decades, small developing states in the Indo-Pacific will have to, not would or could, pick the side (path for their economic and thus humanitarian growth) of either authoritarian or democratic alignments.

Also, technological advancement with the unstoppable race for innovation dominance across the globe is "entwined with evolving geopolitics in the Indo-Pacific as well as the ever- present US-China competition"[38]. A Chinese civil-military fusion, economic-technological espionage, intellectual property theft, development of new forms of military technology (lethal autonomous weapons systems, LAWS), and artificial intelligence are all at the same time a value competition. NATO is aware of that and calls for future legal infrastructure where the law of armed conflict would solve legal dilemmas of responsibility of so-called "robot soldiers", and applicability and adaptability of international humanitarian law to the new era of warfighting – an irregular, hybrid, where peace and war are hard or even impossible to determine.

Last but not least, climate change is a major threat while not only an environmental crisis for the Indo-Pacific nations. The four low-lying atoll nations and territories of the Marshall Islands, Kiribati, Tuvalu, and Tokelau are projected to lose most of their land by the late 21st century, from sea level rise up to three times the world average (Becker et al. 2011). The islands and islanders of the Pacific are the world's climate change frontline. They contribute the least to global warming but are set to suffer the most from its effects, and they now undergo challenging local trial runs for a global future severely impacted by global warming. Again, ocean change poses a global disruption to the stability and prosperity of states, where the most powerful are able to combat the effects of sea-level rise, while the least developed won't adapt. They simply have no means to manage natural and anthropogenic disasters. Therefore, they will be entirely dependent on external aid. Yet,

[34] Chapter 2, Paragraph 2.1(10) of the NATO Strategic Foresight Perspectives Report.

[35] The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is a free trade agreement (FTA) originally signed on March, 8th 2018 between 11 states (thus also called TPP11): Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore and Vietnam.

[36] The Regional Comprehensive Economic Partnership (RCEP) is also a FTA signed on January 1st, 2022 between 10 member states of the Association of Southeast Asian Nations (ASEAN) being Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam, and its 5 FTA partners: Australia, China, Japan, New Zealand and Republic of Korea.

[37] Chapter 4, Paragraph 2 of the NATO Strategic Foresight Perspectives Report.

[38] Chapter 3, Paragraph 2 of the NATO Strategic Foresight Perspectives Report.

as remains obvious, aid does always come at a price. Australian, Japanese, Korean, American, and New Zealand's humanitarian aid programs for the Asian and Pacific nations are directed at the development of those states who will then become more democratic, prosperous, and in the end more reliable politically alias and economically speaking, more solid partners with stabile and open (for the donors, of course) markets. China, in turn, in demand of strategic materials, natural resources, and raw materials lying in the Indo-Pacific area, has been using its engineering projects and at the same time utilizing the Chinese diaspora [extending 15 million] as a soft power instrument to increase its influence in the region. The PRC's "rejuvenation" project intends to transform the country's present status into a wealthy and powerful global power. Yet, "countries who depend on China to pursue economic alternatives will face stagnation and/or potentially political crises[39]".

V. Conclusion

This article proves how the Indo-Pacific region and all the intertwined elements of its security architecture affect the Alliance. Although only two NATO members, the US and Canada, lay at the Pacific Ocean, while the other two have their overseas territories there – the United Kingdom and France, the geopolitical and military importance of this basin is indisputable. NATO's approach to this region yet remains focused on indirectly deepening strategic contacts with its four Asia-Pacific partners: Australia, New Zealand, the Republic of Korea, and Japan. Though the Alliance will remain vigilant for a potential military crisis against the international rules-based order, stability, and its values of democratic, prosperous, and safe nations. The Euro- Atlantic safety and stability do not only rely on its own security architecture but are challenged by multilayered threats and political-economic-military competition with authoritarian regimes from outside of its region. With the rise of China and its aggressive interference in domestic relations of the Indo-Pacific nations, Russian imperialistic hunger which never waned, and other regimes and dictatorships across the world, the Alliance must be able, ready, and well-equipped to protect its values regardless of where a threat comes from. What cannot be forgotten either is the political- military power to counter climate change effects, as ocean change in the Indo-Pacific region has and will continue to lead to demographic instability, mass migration, legal questions of sovereignty and territorial integrity, and thus uncertainty of the world order. Therefore, there is a place for NATO to play a crucial, that is proactive, role in this region reducing the already existing threats to the Alliance, thus the Western civilization's system of values at times of great power competition.

References

Becker M. et al. (2011) *Sea level variations at tropical Pacific islands since 1950* [in:] "Global & Planetary Change" vol. 80-81.

[39] Scenarios, Paragraph 14 of the NATO Strategic Foresight Perspectives Report.

Lipton Eric (2022), *Secret data, tiny islands and a quest for treasure on the ocean floor*, [in:] "The Japan Times", 30/08/2022.

Malhotra A. (2023), *Is India the Balancer in the Indo-Pacific?* [in] InkStick (24.04.2023): https://inkstickmedia.com/is-india-the-balancer-in-the-indo-pacific/

McDonald Scott D. (2023), 战略竞争*? — Strategic Competition?* [in:] *China's Global*

Influence: Perspectives and Recommendations, Scott D. McDonald and Michael C. Burgoyne (eds.), APCSS, Honolulu.

MISEREOR, Bischöfliches Hilfswerk MISEREOR e.V. (2016), *Deep Seabed Mining Treasure chest or another Pandora's box? In focus: the Pacific,* Aachen, March.

Naidu G.V.C. (2001), *India and the Asia-Pacific Balance of Power* [in:] Strategic Analysis: A Monthly Journal of the IDSA, July 2001 (Vol. XXV No. 4): https://ciaotest.cc.columbia.edu/olj/sa/sa_july01nag01.html

Ross Robert S. (2018), *What Does the Rise of China Mean for the United States?* [in:] *The China Questions: Critical Insights into a Rising Power*, Jennifer Rudolph and Michael Szonyi (eds.), Harvard University Press, Cambridge, MA.

Sakellariadou Fani (2022), *Seabed mining and blue growth: exploring the potential of marine mineral deposits as a sustainable source of rare earth elements (MaREEs) (IUPAC Technical Report)* [in:] "Pure and Applied Chemistry", 94/3.

Siekiera Joanna (2022a), *Introduction: The Concept of the West (the European Continent) As a Political Unity*, [in:] *Unity in pluralism: Europe's underestimated strength*, Joanna Siekiera (ed.), CBPE, Warsaw.

Siekiera Joanna (2022b), *Legal aspects of Multi-Domain Operations*, [in:] "The Magazine of the NATO Rapid Deployable Corps – Italy" 33/2022.

Spalding M.J. (2011). *Perverse Sea Change: Underwater Cultural Heritage in the Ocean is Facing Chemical and Physical Changes* [in] "Cultural Heritage and Arts Review", 2(1).

USNI News, *Report to Congress on Chinese Naval Modernization* (17.05.2023): https://news.usni.org/2023/05/17/report-to-congress-on-chinese-naval-modernization-17

MARITIME CRITICAL INFRASTRUCTURE PROTECTION (MCIP) IN A CHANGING SECURITY ENVIRONMENT[40]

Diren DOĞAN[41] – Deniz ÇETİKLİ[42]

Preface

The twenty-first century represents the most advanced point in human history considering all the technological and social changes. Societies have developed around geographical features, natural resources, technological progress, and cultural values and have reached their current position. From the invention of the wheel to the Industrial Revolution, from the invention of writing to the beginning of the Internet age, developments inherited from the past have affected lives and made them easier. However, the convenience of everything carried for generations has increased dependence on them and brought new threats. The security of nations and their overall functioning of the international system are all under attack today from diverse types of threats, including physical, cyber, and hybrid. And the most sensitive points of these attacks are critical infrastructure which refers to facilities, systems, and networks that are vital to the functioning of a society. Another feature of the twenty- first century is that it is a "grey century" characterized by complexity. This situation results in the emergence of unpredictable threats, the origins, characteristics, and consequences of which are unknown and cannot be predicted and can affect multiple areas simultaneously. The maritime environment is important for various critical industries such as communication, transportation, energy transfer, trade, etc., and is vulnerable to these types of threats due to the world's increasing interconnectedness through globalization. The threats faced by this gigantic "blue economy", targeting the sustainable use and management of ocean resources for economic growth, job creation, and the overall well-being of society. The oceans cover about 70 percent of the Earth's surface, and they have a significant impact on global trade, with more than 80 percent of the world's trade being transported by sea and show the importance of the seas for the continuity of the global economic system, while revealing how sensitive knots maintain the existence of an interconnected world in every respect. In this direction, this study aims to address the protection of "Maritime Critical Infrastructure", understood simply as the systems and assets that are essential for the functioning of a society, economy, and country from a maritime perspective. In this context, the concept of critical infrastructure will be discussed first, and then the role of maritime critical infrastructure, the risks faced by critical infrastructure, and what needs to be done to ensure resilience will be discussed under different sub-titles. Considering the above framework, the sources used were primarily the workshops conducted by the

[40] *This Study Paper was prepared for MARSEC COE's MCIP Project and presented at the 3rd Maritime Security Conference.*

[41] *PhD Candidate in International Relations is a lecturer in Alanya Alaaddin Keykubat University, International Relations Department. diren.dogan@alanya.edu.tr*

[42] *Commander Turkish Navy-OF-4, Weapons of Mass Destruction (WMD) Staff Officer of MARSEC COE, İstanbul/Türkiye wmd.cdbranch@marseccoe.org*

NATO Maritime Security Centre of Excellence (MARSEC-COE) in 2021 and 2022, publications produced by NATO Centres of Excellence, relevant NATO, and academic publications. All this is to produce a study paper written on a framework used to clarify the notion of what constitutes Maritime Critical Infrastructure, which makes consistent use of MARSEC-COE's work done in this respect so far.

Special Note: The study paper published in October 2023 and can be downloaded from the link **https://www.marseccoe.org/published-work/**

OFFSHORE CRITICAL ENERGY INFRASTRUCTURE: A MARITIME SECURITY PERSPECTIVE

Dr. Nicolas MAZZUCCHI,
Research Director, Centre d'études stratégiques de la Marine (CESM), French MoD
nicolas1.mazzucchi@intradef.gouv.fr

The development of offshore electricity production, mostly using wind turbines, and energy transmission networks – subsea gasoducts and power transmission lines – in an ongoing phenomenon in Europe for more than 20 years now. Moreover, the pace is accelerating, as the sea appears a major territory for the energy transition, in terms of resources as well as a transit area for energy. The importance of these infrastructures, representing an important part of the energy sector in certain European countries such as Denmark – more than 25% share of offshore wind in the national electricity production – tends to consider them as critical assets in terms of energy security.

Yet the sea could also be considered a very interesting territory for gray zone actions and hybrid warfare. The contestation of international law, with a growing number of countries challenging the provisions of United Nations Convention on the Law of Sea (UNCLOS), the opacity of the underwater domain, allowing special forces actions difficult to attribute, and the overlapping of public and private interests beyond national waters, may help proxies and state-sponsored actors to provoke disruption and to develop specific strategies towards offshore critical energy infrastructure.

Therefore, armed forces and MODs should develop specific orientations to counter these threats and to help mitigating the effects of a direct action, whether kinetic or cyber, towards offshore critical energy infrastructure. The French Navy organization, using military forces for State Action at Sea and not having a separate force of coast guards, helps to deter and prevent this kind of action. Maritime security could also be fostered in Europe and beyond, in strengthening further the cooperation at a multi-stakeholder and multi-lateral level.

I. Offshore Critical Energy Infrastructure development: a historical perspective

Energy transition is a major trend in all NATO nations with national specific orientations. Yet one common point exists among all national policies: the reinforced role of the sea both as a territory for energy production, using offshore wind mostly, and as a territory for energy transit. The need to phase out from coal and oil, oriented the energy consumption in NATO countries towards both gas and low-carbon electricity. To support this transition, following the international negotiations on climate from 1997 on, gas-rich countries in Europe and North America invested in gas exploration-production both onshore and offshore. In Northern Europe in particular, namely Norway and the UK, the development of gas production occurred mostly at sea with an increased number of offshore gas platform, following two directions: northward towards the Arctic and farer from the shore, with the decrease in deep and ultra-deep offshore gas productions for 30 years. Nowadays, this trend continues, notably in Norway, with recent discoveries of exploitable gas deposits in Barents Sea and Norwegian Sea, the exploitation of gas is ever closer to the North Pole and even farer from the shore with some discoveries reaching the borders of Norway's EEZ. Together with offshore gas production in Northern Europe, as well as potential offshore gas production in the Eastern Mediterranean, the offshore energy production is also a matter of renewable energy sources, mostly offshore wind. Baltic countries such as Denmark and Germany, alongside Atlantic countries (the UK, Spain, the US, France, etc.) developed for years important offshore wind parks, to benefit from the decrease in electricity production costs from wind and further decarbonize their national energy sector, consistently with environmental regulations. In Denmark, around 30% of electricity generation is nowadays made using offshore wind farms[43], the country also benefitting from its offshore interconnection with Norway and Sweden to access their cheap hydropower surplus. Between 2013 and 2022 the capacity of offshore wind in Europe grew more than 4 times, from 7 GW to 30 GW installed[44]. Moreover, the RePowerEU plan of 2022 also advocates for a strong development of offshore wind in the EU, to accelerate the transition and free Europe from the need to import massive volumes of gas from Russia. Yet, as the renewable energy sources are not pilotable facilities, their growing share is having an impact on electric networks, causing a more complex equilibrium demand-offer to balance, therefore transferring the security of supply from the electricity producers to the network operators[45].

Regarding gas, the continuous development of the use of gas has a strategic consequence: the development of networks and infrastructure at sea, to transport gas in gaseous or liquid state to Europe and NATO countries. Liquefied natural gas (LNG) regasification terminals were at the core of energy decontinentalization, following the decision to stop importing gas from Russia. European countries that were developing for years the regasification capabilities, were fortunate to have operating LNG terminals able to accommodate LNG coming from new or already existing sources (Qatar, the US, Algeria, etc.). Before 2022, gas supplies in Europe mostly came through land routes, with Russia alone accounting for 40% of imports. In early 2023, gas supplies are a maritime issue, with the role of Mediterranean, Atlantic and Gulf countries. With the progressive stop of gas imports from Russia, alongside the continuous development of gas use in Eastern Europe to phase-out from coal, maritime gas supplies should continue to grow, at least in the near future. Therefore, European countries and Turkey are considering the acquisition of new LNG terminals to increase the import of LNG, thus reinforcing the importance of the sea – Mediterranean, Atlantic and Baltic – for hydrocarbons supplies[46].

Nowadays in Europe, offshore critical energy infrastructures are a critical part of the continent's energy security, in providing electricity production capabilities as well as major network interconnection. The attack

[43] 28.2% in 2020 according to IRENA statistics.

[44] Wind Europe, *2022 Statistics and the Outlook for 2023-2027,* Wind Europe, 2023.

[45] The 2021 Security Report from the French TSO RTE highlights this issue (p. 11) : RTE, *Bilan sureté 2021,* Paris, RTE, 2022.

[46] IEA, *How to Avoid Gas Shortages in the European Union in 2023*, Paris, IEA, 2022.

on Nord Stream 1 & 2 attracted the attention over underwater gas transportation networks, yet the major issue should be more on electricity transportation rather than on gas. As the attack on Nord Stream demonstrated, the destruction or the paralysis of a major gas transportation infrastructure leads to a disruption on gas supplies for the end-customers and therefore have a major impact on energy security and on market prices. However, apart from this disruption and the immediate effect caused, there is no major break in the continent's energy supplies as gas could be re-routed through other means, whether gasoducts or LNG carriers.

On the contrary, for electricity transportation networks the situation appears fundamentally different, as an electric network has to maintain a permanent balance between production and consumption. In the hypothesis of a major electric line failure, the cascading effect may cause a major blackout on the network if no backup solution could be put online in a short time. Electric transmission systems operators (TSO) usually can dispatch electric fluxes through different sub- networks or alternative routes and possess backup capabilities to maintain the balance within the fault tolerance margins of the network. Yet, considering a major failure or the failure of enough major electric lines at the same time, there is a significant risk that a cascading effect could cause a major blackout, especially considering the ongoing integration of electric networks in Europe. To support and strengthen the integration of networks, especially the connection between synchronous grids (European Continental, Nordic, Baltic, Great Britain, Ireland), transmission system operators developed power cables interconnexions. Consistent with the EU policy of energy integration, following the 3rd Energy Package of 2009 (aiming for 20% of cross-border electricity interconnexion)[47], European countries developed their integration with transnational power lines, including underwater. Since 2000, many major power lines have been built, with a specific focus on the Baltic (SwePol in 2000, Skagerrak-4 in 2019, EstLink 1 & 2 in 2006 and 2014, NordBalt in 2014, etc.) and the Channel/North Sea (BritNed in 2009, COBRACable in 2016, Nemo-Link in 2019, etc.). They create nowadays a dense network of subsea electric cable, crossing the Baltic straits and allowing a better integration. Yet with the sabotage of Nord Stream gas pipeline in 2022, this electric network appears today both as an important feature for European integration, as well as a majority vulnerability for the continent's security.

II. Impact on military operations and activities

The development of offshore critical energy infrastructure in Europe and North America had direct impacts over military operations and activities. Renewable energy sources, especially offshore wind turbines create electromagnetic fields that may disturb the function of radar and air defense systems installed in coastal areas. The UK MoD and the EDA at an EU level therefore organized multistakeholder working groups[48], with wind

[47] Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) No 1228/2003 : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02009R0714-20150105

[48] Example from the UK MoD : Mitigating the adverse effects of offshore wind farms on air defence radar: concept demonstrations : https://www.gov.uk/government/publications/mitigating-the-adverse-effects-of-offshore-wind- farms-on-air-defence-radar-concept-demonstrations/mitigating-the-adverse-effects-of-offshore-wind-farms-on- air-defence-radar-concept-demonstrations

turbines manufacturers, radar and warning equipment manufacturers, armed forces, and ministries in charge of energy to elaborate solutions regarding the geographical location of future wind parks as well as to work on radar systems and materials in the wind turbines, in order to lower as much as possible, the impact of their development over military activities. With the growing extend of offshore wind parks, from a dozen MW to more than 1 GW planned in the Straits of Sicily, the size of the infrastructure to protects grows accordingly. The distance between two 15 MW wind turbines, in order to have the maximum electricity output, could not be inferior to 1000 m.

Moreover, any offshore major infrastructure, such as gas rigs or high-power wind turbines, is having a dedicated subsea architecture from the surface to the seabed. These cables or jackets also create a dense metallic subsea network that could have an impact over antisubmarine warfare missions and the detection of submarines, allowing potential opponents to use them for hiding. Alongside the effect on sensors, especially on coastal air-awareness radar, their potential impact over coastal military activity could be dramatic, considering also their rapid development all over NATO countries, especially in Northern Atlantic and the Baltic.

The need to protect them, considering their criticality for any national energy system and power grid, leads to a reinforced involvement of armed forces, especially navies in both situation awareness and direct protection against kinetic or cyber threats. As a major failure in gas or electric network may have tremendous consequences for both military and civilians, especially in case of major blackout, the protection of these infrastructure tends to become a critical mission for the armed forces, especially the navies and the entities in charge of defensive cyber operations.

The vulnerability of energy infrastructure to cyber-attacks, especially renewable energy production facilities such as wind farms[49], forced the national and multilateral regulators to have a specific look on dedicated regulations. In the EU, the NIS (2016) and NIS 2 (2022) Directives[50] strengthened the requirements in terms of cyber-protection for any critical entity whether national or transnational. These directives give the national entities in charge of cyber-protection and the enforcement of regulations regarding cyber-security, important powers to support the companies possessing these offshore critical infrastructures in developing their resilience to cyber-attacks. In some EU countries, even if the administration in charge of cybersecurity doesn’t belong to the military – in France for example, the ANSSI is not an MoD-related organization but is over direct supervision of the Prime Minister’s Office – the civil-military cooperation, in terms of intelligence

[49] N. Mazzucchi, « Renewable Energy Infrastructure: Physical and Cyber Vulnerabilities Assessment », *Operational Highlights* n°12/2019, pp. 32-38.

[50] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) : https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:32022L2555

sharing and situation awareness regarding the cyber threats is a permanent feature. The very same civil-military cooperation could be found also outside the EU, in the US for example, with a direct support from the DoD to the DHS regarding the protection of any critical infrastructure, especially related to the defense sector. Cyber-task groups, permanent cooperation forums or platforms are therefore a common feature nowadays in NATO countries, with for some years, a specific look on what could happen at sea, considering the whole digitalization of maritime industry and the development of offshore critical energy infrastructure.

Alongside cyber-protection, the armed forces are also engaged in direct physical protection, as they become critical in the stability of national and continental energy networks. A direct attack over subsea power cables under the Baltic, from Sweden and Norway to Denmark for example, may cause cascading effect in both interconnected electric networks in Continental Europe and Scandinavia, resulting – if the reaction from the TSO and TSO associations is not swift enough – an unprecedented blackout. Power cables linking two transmission systems are not the only ones to consider as the development of offshore renewable energy production facilities, mostly wind but also tidal turbines in the Northern Sea, need to be linked to the electric substations ashore through power cables. Therefore, alongside the major power cables, having more than 100 MW of capacity, a myriad of low and mid-tension power cables exists at sea from the renewable offshore infrastructure to the national transmission and distribution networks. Considering their power capacity, their failure is less prone to provoke a blackout, yet they are far less protected than the high-capacity ones.

Gas infrastructure, especially those using LNG are therefore considered hazardous facilities, covered by the SEVESO III regulation in the EU[51]. A direct kinetic attack over an LNG terminal could therefore cause major damages to neighborhood and have a direct cognitive effect over the population. Moreover, the fast-paced development of offshore wind farms also creates new surface of vulnerability as the wind turbines have not been conceived to resist direct kinetic attacks – contrarily to nuclear powerplants for example – and the perimeter security of offshore wind farms, considering the size of the plant, is particularly difficult. Moreover, the development of gas rigs, offshore wind farms is also eloping farther away from the shore, lead to an increase in security costs as it is particularly difficult to intervene in high seas in case of a major security incident, transferring the security management from private contractors to armed forces.

These risks must be considered first from a symmetric point of view, especially with the growing international tension at the borders of NATO, but also from a hybrid warfare point of view. Hiding the identity of the attackers and acquiring the capabilities to provoke a major failure in any of these infrastructures could be relatively easy, creating the perfect background for state-sponsored attack using false-flag operation or proxies.

[51] Directive 2012/18/EU : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018

III. Countering hybrid warfare on energy infrastructure

At a technical level, the national companies and European association for transmission of electricity – ENTSO-E for the EU – could disconnect certain parts of an overloaded network due to a failure, to avoid the cascading effect. Yet, a major coordinated attack on a certain number of major electric subsea cables, in the Baltic for example, could be serious enough to overcome this network management solutions, especially considering cross-border effects. As of 2021, a large part of EU countries didn't have electric capacity mechanisms nor interuptibility schemes, especially for the countries belonging to the Nordic and the Baltic pools[52]. Considering the geographical issue of the Baltic, underlined by the attack on Nord Stream 1 &2, there is a relative ease to commit direct subsea action at a low-mid depth, were a large part of subsea cables are. Even if national or continental entities are acting to prevent major energy crises – such as the EU with the 2019 Regulation on risk-preparedness in the electricity sector[53] - most of them address the hypothesis of a natural disaster or a local attack on a facility or a network. The hypothesis of a major coordinated state-sponsored attack, even caused by a proxy actor, appears very difficult to foresee at to prevent against.

Armed forces should therefore develop capabilities and capacities to monitor and assess major risks of attacks on these offshore energy critical infrastructures as the private security companies may not be the relevant level of protection in case of a hybrid warfare attack. NATO nations navies should consider reinforcing their monitoring of offshore critical energy infrastructure development as the critical orientation of these infrastructures will continue to develop in the future. Adequate organization and dedicated policies and doctrines are compulsory to address this growing risk of an attack causing major damages.

The French Navy organization and doctrine is therefore useful considering the need to counter and – if possible – deter any hybrid threat. The French Navy is responsible for all sovereign actions at sea, including the protection of energy assets, as France chose not to a create a separate corps of coast guards. State Action at Sea, including the fight against seaborne trafficking, the protection of environment and law enforcement regarding INU fishing, is therefore directly done using navy assets, with a military chain of command. Consequently, there is no "administrative grey zone" that could be used by a hybrid opponent to take advantage of. Navy frigates are therefore used against non-state actors and the difference between State Action at Sea missions – considered as law enforcement missions – and combat missions is a matter of orders and minutes. Thus, this organization helps to shorten the OODA loop, giving an advantage for reacting to any hybrid warfare action targeting offshore energy critical infrastructure.

[52] ACER, *Security of EU electricity supply in 2021: Report on Member States approaches to assess and ensure adequacy*, Brussels, ACER, 2022.

[53] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC : https://eur-lex.europa.eu/legal- content/EN/TXT/PDF/?uri=CELEX:32019R0941

Another major solution is the civil-military cooperation. As highlighted in Norway, the navy may not have enough capabilities to survey on a real-time basis any offshore infrastructure. Yet the private and public companies owning the gas rigs or the offshore wind farms are themselves confronted to the need of having the ability to monitor the status of subsea parts, to avoid any major failure caused by corrosion for example. Thus, for more than ten years now, considering the development of offshore infrastructure, they decided to supplement the traditional divers, in charge of such a monitoring, with unmanned underwater vehicle (UUV) able to detect and, for some of them, to have a direct action. Oil & gas was the very first business to engage in the robotization of subsea monitoring at a large scale, explaining that most of UUV manufacturers were at first oil and gas suppliers, before turning to the military customers.

Therefore, considering the importance of offshore energy in Norway – with nowadays more than 500 UUV active in public and private companies - the country decided to promote a public-private partnership to support information and intelligence sharing between the energy companies operating UUVs and the military, for the navy to access information and improve situation awareness[54]. Considering the development of seaborne energy issues, including the transportation of liquified gas to Europe, the cooperation between civilian and military entities is a key for improving the security at sea. In France, since 2016, the French Navy operates the MICA Center (Maritime Information Cooperation and Awareness Center)[55] whose role is to support the naval voluntary cooperation, in centralizing the information on any maritime security incident, at first along the shores of Europe and nowadays with a global extent. The MICA Center centralizes the information from any shipowner or operator and provides security warnings from the French Navy and the European partner navies participating to the center (Spain, Portugal, Belgium), with a specific focus on the Gulf of Guinea and the Horn of Africa. The combination of these cooperations, close to the shores with the UUV operators and the information sharing in high seas, may provide at a NATO level a global network of intelligence sharing and gathering to detect and counter any hybrid threat at sea.

Alongside these dedicated policies to face kinetic attacks, there is the need to reinforce the cyber- protection of these infrastructure as they are ever more relying on industrial control systems such as SCADA for the piloting of the facility. Certification of cybersecurity products for industrial piloting, participation to major exercises for cyber-crisis, multi-stakeholder information sharing forums, are needed to ensure the best level of cybersecurity possible. Here again, there is the need to avoid any stovepipe effect and to associate the highest number of stakeholders possible, including armed forces, NATO and the EU, to ensure a better coordination for response.

[54] Presentation from Rear-Admiral, R. Andersen, Chief of Staff Norwegian Navy, at the First Sea Lord Sea Power Conference (2023 May 16th, London).

[55] https://www.mica-center.org/

IV.Conclusion

The sea is becoming the new major territory for energy production and transportation. Alongside oil and gas for which the deep and ultra-deep-water exploitation are a major feature of the sector for almost 30 years, new developments reinforce the importance of sea and subsea domains. Energy transition all over NATO countries, with the implementation of offshore renewable electricity production facilities, alongside the strengthening of subsea cross-border electric interconnexions in the Mediterranean, the Atlantic and the Baltic, creating a whole electric subsea network, change the energy landscape in Europe and North America. Yet, with this transition comes new security risks as the attack on Nord Stream gas pipelines demonstrated in 2022. The importance of offshore critical energy infrastructures, including LNG terminals, for the energy sectors of NATO countries make the sea a major area to monitor as minor or major coordinated attacks – kinetic or cyber – could have tremendous effects.

Therefore, the reinforcement of situation awareness and the need for NATO navies to consider ever more the offshore energy sector as a major element to protect and to deal with, are compulsory. In the same time, multi-stakeholder cooperation for physical security as well as for cyber-security are the key to avoid a hybrid warfare attack that would benefit from an administrative grey zone to cause major damages. As for any military operation, there is the need to accelerate the OODA loop, having from the beginning an appropriate organization and well- established procedures. Thus, this issue of the protection of offshore critical energy infrastructure is a perfect area for NATO-EU cooperation.

Author CAPT Daniele RUGGIERI Italian Navy General Staff
Head of Submarines R&D Office (daniele.ruggieri@marina.difesa.it)

I. Interests and threats into the underwater operating environment.

The underwater portion of the maritime domain is acquiring a growing relevance thanks to the variety of interests it hosts. At the same time, the technological advance, making even the deep-sea floor accessible, is exposing those interests at growing risks.

Starting from telecommunication systems, today's economies are highly reliant on the global **information technology infrastructure**, with 99 percent of intercontinental communications moving through undersea cables, most of which lack even basic defenses[56]. These cables play a crucial role in enabling international data transfers, including internet traffic, telecommunications, financial transactions, and more[57]. While undersea cables are essential for global connectivity, it is important to ensure their security and resilience against potential threats. Protecting these cables is crucial, as disruptions or damage to them can have severe consequences, including communication breakdowns, financial losses and consequent economic instability.[58]

Furthermore, the exploration, extraction, and transportation of **gas, oil, and other energy resources** at sea involves inherent risks and challenges. Offshore energy operations also involve shipping and transportation of energy commodities. Hybrid threats, which encompass a combination of conventional and unconventional tactics, can pose significant challenges to commercial entities operating in the energy sector[59]. These threats may include piracy, terrorism, cyber-attacks, and sabotage, among others. Safeguarding this wide set of critical infrastructure, including pipelines, offshore drilling platforms and liquefied natural gas (LNG) terminals[60], is crucial to maintaining the reliability and security of energy supply chains.

Besides telecommunication cables, **underwater power cables** have gained significant importance and are becoming increasingly critical in various sectors. With the anticipation of a green revolution and the focus on harvesting alternative energies, submarine electricity cables are indeed expected to gain prominence as umbilical cords to future offshore energy parks. As the world seeks to transition to cleaner and more sustainable energy sources, offshore wind farms, tidal power plants, and wave energy converters are being developed in coastal and offshore areas. These renewable energy installations need a reliable and efficient means of transmitting the electricity generated back to the mainland power grids. Therefore, underwater power cables play a vital role in connecting these offshore energy installations to the onshore power infrastructure.

[56] Undersea Cables: The Great Data Race Beneath the Oceans | ISPI (ispionline.it)

[57] Undersea Cables and the Challenges of Protecting Seabed Lines of Communication | Center for International Maritime Security (cimsec.org)

[58] Invisible and Vital: Undersea Cables and Transatlantic Security (csis.org)

[59] NATO Review - Energy security in the era of hybrid warfare

[60] Global Gas Infrastructure Tracker - Global Energy Monitor

They serve as the primary means of transmitting the electricity generated from renewable sources, such as wind, tide or wave, to the onshore grid for distribution to consumers.

All these infrastructures are designed to withstand the harsh marine environment, including exposure to saltwater, strong currents, and potential impacts from marine life and other elements. They are engineered to be highly durable, reliable, and capable of efficiently transmitting data or high-voltage power or delivering energy resources over long distances. The installation and maintenance of underwater infrastructures pose significant technical challenges. Specialized vessels and equipment are required for laying and burying equipment on the seafloor, often at considerable depths. Additionally, regular inspections and repairs may be necessary to ensure an uninterrupted service or avoid leakages with environmental damage in case of pipelines.

There are two primary forms of attack on undersea critical infrastructures, each of which involves unique threats relevant to the countries[61]. The first is a traditional physical attack, such as explosions or severing of cables, which may be carried out by a state or non-state actor or caused unintentionally by commercial activities such as shipping and fishing, or by extreme weather or earthquakes. In the case of accidental damage, private entities bear the primary responsibility for mitigating these threats. In the case of a malicious attack, an adversary may use surface vessels or submarines to deploy manned or unmanned equipment capable of disrupting or destroying undersea cables or pipelines. The second form of threat comes from the cyber domain, with cyber-attacks to communication infrastructure, aimed at disrupting the service or stealing data for espionage purposes[62], or to management systems of energy infrastructures.

The likelihood of physical damage or cyber-attack to such equipment has increased rapidly in recent years, due to technological development especially with the proliferation of subsea technology. Enhancing maritime security through measures like vessel tracking systems, maritime patrols, and cooperation with naval forces can help mitigate risks associated with piracy and other maritime threats. Collaborating with relevant stakeholders, including governments, international organizations, and industry partners, is important for sharing information, best practices, and intelligence regarding potential threats and mitigation strategies. This cooperation can enhance the overall security posture of offshore energy operations. It is worth noting that regulations and industry standards play a significant role in ensuring the security of energy supply chains. Governments and regulatory bodies often impose specific requirements on energy companies to enhance security measures and promote safe operations. In this field specific attention should be given to the security of pipelines, strategic infrastructures running for thousands of kilometers on the seafloor taking into consideration that the natural protection of hundreds or even thousands of meters of water column above them is no longer enough to ensure their security against modern threats[63].

[61] Security threats to undersea communications cables and infrastructure – consequences for the EU (europa.eu)

[62] How a US Navy Submarine Secretly Tapped Russia's Undersea Cables | The National Interest

[63] Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies", G. Soldi, C. Warner and

By implementing robust security measures, conducting regular risk assessments, and fostering collaboration, private companies can work towards safeguarding critical offshore infrastructure and maintaining the reliability and security of energy and data supply chains.

Overall, governments and private entities involved in operating and maintaining underwater critical infrastructures must invest in robust security measures to safeguard them against physical and cyber threats.

Moreover, the seabed is reach in energy and mineral resources, therefore it represents a new frontier, especially for minerals and rare-earth elements, for the sustainment of modern societies. The underwater environment is also incredibly rich of genetic resources and a source of bio- diversity making it, again, essential for life on the surface. Finally, the seabed can offer the solution to store the excess of carbon dioxide produced by human life above the surface. All of these considerations make it clear how important the portion of the world that lies below the surface of the sea is to humanity[64].

II. Why the underwater operating environment is worth to be recognized as a new operational domain?

Italy is home to critical infrastructure located in coastal and marine areas, making the underwater environment a crucial part of its infrastructure resilience. Coastal and marine areas in Italy host a range of critical infrastructure, including ports, oil and gas facilities, underwater pipelines, and communication cables. These infrastructures are essential for the country's economic growth and development, making their protection and resilience essential for the well- being of the nation.

Given its relevance, the underwater portion of the maritime domain is emerging as a new arena of competition for international players, with their interests centered on effective access to and exploitation of this environment. Largely unexplored, the underwater environment has such peculiar physical characteristics that it requires the use of specialized tools, technologies and communication means totally different from those used in other domains[65]. This uniqueness has pushed the exponential growth of underwater technologies that is making remote underwater locations more accessible for various human activities. However, this accessibility may also attract the attention of criminal or terrorist activities, posing potential security threats.

Recognizing the evolving nature of this environment, the Italian Navy is progressively adopting a new approach by promoting the definition of the **Underwater Domain as a distinct operational domain**[66]. This domain can be considered as the fifth physical dimension, alongside the traditional domains of land, sea, air, and space.

others, 3 Feb. 2023

[64] https://www.un.org/en/chronicle/article/international-seabed-authority-and-deep-seabed-mining

[65] ACMv2.pdf (rutgers.edu)

[66] ITA National elements at AJP 3.1

Recognizing a new underwater domain can help address its peculiar vulnerabilities and leverage its specific strengths within a multi-domain approach. In addition, fostering knowledge sharing and collaboration among different domains and stakeholders is crucial.

By acknowledging the unique challenges and opportunities presented by the underwater environment, the natural consequence is to develop strategies, technologies, and capabilities tailored to operate effectively in this domain. This may include advancements in underwater sensing, communication, surveillance, and security systems, as well as specialized training for personnel operating in underwater scenarios. Indeed, it is essential to establish seamless integration and interoperability between the submarine domain and other domains such as air, land and space in order to ensure effective coordination and communication between different domains, maximizing the potential for collaborative actions and information sharing. The collective effort promotes innovation, efficiency, and the maximization of potential benefits within the underwater domain. By considering these factors and implementing appropriate strategies, recognizing and effectively exploiting a new underwater domain will significantly enhance operational efficiency and coordination in a multidomain context.

Focusing on doctrine, a new domain requires an innovative approach to military operations that shall consider underwater warfare[67] as a whole; it has to unify the anti-submarine, mine and seabed warfare with a common and essential reference infrastructure represented by the underwater situational awareness (UWSA).

III. Capability development for the underwater domain.

The recognition of the Underwater Domain highlights the need for a comprehensive and multidimensional approach to maritime security, encompassing both traditional surface operations and the increasingly significant underwater component. This shift in focus aligns with the evolving nature of global security challenges and the need to adapt to emerging threats in a rapidly changing world. This includes the development of a seabed strategy that requires the need to reach deep sea to operate on energy pipelines, communication lines and offshore infrastructures. Operating on the seabed requires the extensive use of unmanned[68] or remotely guided underwater vehicles that the Italian Navy is already able to deploy through its conventional naval platform[69]. In response to the sabotage of the Nord Stream pipelines and to ensure the surveillance of national strategic submarine infrastructures, the "Operation Fondali Sicuri[70]" has been launched, employing Mine-hunting assets, special diving equipment and other specialized assets[71].

[67] Peters, Johannes, "Below the Surface: Undersea Warfare Challenges in the 21st Century", 2021/01/01 https://www.researchgate.net/publication/352960209_Below_the_Surface_Undersea_Warfare_Challenges_in_the_21st_Century

[68] Unmanned Underwater Vehicles: Defence and Technology Trends (naval-technology.com)

[69] "Future Combat Naval System 2035" concept_ver11 (difesa.it)

[70] *Fondali sicuri*" states for "safe seabed".

[71] Operation Safe Mediterranean: handover of the tactical command to Taranto - Online Defense (difesaonline.it)

However, **further advancements are needed in the field of unmanned vessels**, underwater sensors and communication systems to access even greater depths with enhanced endurance and autonomy and to ensure an extensive surveillance of the underwater domain. Indeed, a safe underwater domain relies on the capability to acquire a reliable and constant **Underwater Situation Awareness (UWSA)**. Given the peculiar physical characteristics of the underwater environment, developing UWSA requires a network of underwater sensors and unmanned vehicles completely integrated with conventional maritime forces such as ships, submarines, Maritime Patrol Aircraft/Helicopters and coastal surveillance systems.

Focusing on unmanned capabilities, the development of **unmanned underwater vehicles (UUVs)** and sensor networks has significant potential to optimize operations in deep-sea environments. UUVs equipped with advanced sensors, robotic arms, and manipulation tools can be deployed for inspection, maintenance, and repair tasks on critical infrastructure such as energy pipelines and communication lines. These vehicles can operate at great depths and in hazardous conditions, reducing the need for human divers and minimizing the associated risks. This not only minimizes the risks associated with human involvement but also improves cost efficiency by eliminating the need for extensive support vessels and manned operations.

Furthermore, they can act as data collection and monitoring sensor networks. Given the last technological development[72], it is possible to apply a new concept of underwater residency, with unmanned capabilities permanently deployed to patrol and monitor underwater installations, detecting and responding to potential threats such as unauthorized access or tampering. With advanced sensor technologies, UUVs can also detect and identify underwater mines or other hazards, enhancing overall safety. Moreover, UUVs equipped with specialized scientific instruments enable researchers to explore and study the deep sea in more detail. Deployed in the deep sea and properly connected to the surface UUVs can provide real-time data on various environmental parameters, including water quality, temperature, pressure, and marine life. These data are crucial for understanding deep-sea ecosystems, detecting changes, and monitoring the health of underwater installations. They can also collect samples, conduct experiments, and capture high-resolution imagery or video footage of deep-sea ecosystems. These advancements in exploration technology help expand our knowledge of the deep sea and its potential resources. In summary, the development of advanced UUVs and sensor networks holds great promise for optimizing operations in deep-sea environments. It enables efficient infrastructure maintenance for the private industry, enhances safety and security, facilitates scientific research and exploration, and improves overall cost-effectiveness. These advancements contribute to a better understanding and utilization of the deep-sea ecosystem while minimizing risks to human life.

Italy has indeed recognized the importance of maintaining control over the underwater domain and protecting its interests. To achieve this, a structured approach that focuses on the development of advanced

[72] Naval Combat Systems: Developments and Challenges | IAI Istituto Affari Internazionali

submarine robotics and technologies is needed. These cutting-edge advancements are driven by industrial and academic excellences, with a relevant research and development effort specifically tailored to meet the operational needs of the Navy. As part of this strategic initiative, Italy is establishing a **National Underwater Center** in La Spezia. This location is significant because it is situated close to the NATO CMRE (Centre for Maritime Research and Experimentation) in order to allow collaboration, knowledge sharing, and leveraging on expertise in underwater research and technologies. The National Underwater Center serves as a hub for research, development, and innovation in underwater robotics and related technologies. It brings together various stakeholders, including industry, academic institutions, and government agencies, to foster cooperation and synergy in advancing Italy's capabilities in the underwater domain. By investing in cutting-edge technologies and establishing the National Underwater Center, Italy aims to enhance its naval capabilities, strengthen its control over the underwater domain, and safeguard its national interests. This strategic approach underscores Italy's commitment to leveraging industrial excellence and research-driven innovation to stay at the forefront of underwater technology development.

IV. Civil-military cooperation and an updated legal framework.

In the context of ensuring the security and integrity of underwater infrastructure and addressing the challenges posed by the growing presence of military vehicles, ships, submarines, and private organizations in the underwater domain, technology and capability development are not enough as standalone measures. Taking into consideration that most of undersea infrastructures are privately owned, it is also essential to develop **collaborations with key players** involved in underwater energy infrastructure and submarine communication cables. ENI, a major energy company, and TI Sparkle[73], a leading provider of submarine cable systems, are among the main partners that have been engaged into collaborations with the Italian Navy. With a joint and shared effort, private companies can increase their own measures and capabilities to detect threats to undersea infrastructures, making possible to Governments and Navies to take action only when and where needed. By working together, the common aim is to enhance the security of critical underwater infrastructure.

In addition to these collaborations, recognizing the steady increase in underwater activities[74], there are initiatives promoting the development of an updated legal framework for the underwater domain. Given the growing importance of critical seabed infrastructure, which encompasses various installations and structures on the seabed, it becomes imperative to establish a comprehensive legal framework to govern and protect these assets effectively. This should include rules for classification and certification of unmanned vehicles operating underwater and the establishment of a unique organization responsible for underwater activities authorization. A sort of **National Underwater Traffic Control Authority** that would be responsible for

[73] Italian Navy and Sparkle Signed Memorandum of Understanding for the Protection of Subsea Telecommunication Cables | Sparkle (tisparkle.com)

[74] Global Submarine Proliferation: Emerging Trends and Problems (nti.org)

managing requests for access to underwater areas and resolving any interference issues that arise between different activities[75]. To effectively manage underwater traffic, the National Underwater Traffic Control Authority would implement horizontal and vertical separation criteria as already implemented with submarines by Allied Submarine Operating Authorities. These criteria would provide guidelines for ensuring safe and coordinated operations, minimizing the risk of collisions or conflicts between different underwater activities. The proper application of these criteria requires that unmanned vehicles have to be classified and certified in order to be able to apply different separations based on vehicles' characteristics. Taking together this measure will contribute to enhance the underwater situational awareness, making possible to conduct anomaly detection on unauthorized activities close to critical infrastructures.

Given the trans-national extension of undersea infrastructures a nation-level approach it is not enough, and countries and international organizations might consider revisiting and expanding the existing international legal framework. This revision could involve the development of specialized regulations, guidelines, and protocols specifically tailored to the construction, operation, maintenance, and protection of critical seabed infrastructure. There might also be the need of specific bi or multi-lateral agreement among nations connected by the same infrastructure. International organizations like the International Seabed Authority (ISA)[76] and regional bodies may play a significant role in facilitating discussions and negotiations among nations to update and strengthen the legal framework in relation to critical seabed infrastructure. Collaboration, cooperation, and the involvement of relevant stakeholders will be essential to achieve a comprehensive and effective legal framework that addresses the evolving challenges in this domain.

Overall, the protection of the underwater domain and its critical infrastructures requires a complete toolkit of measures that can be grouped as follows:

- accelerating technology and capability development.
- renewing civil-military cooperation.
- promoting a new legal framework at national and international level.

These measures align with the responsibility of governments to safeguard critical infrastructure and to ensure the protection of national interests in the underwater domain.

V. The proposal of a NATO Underwater COE.

The relevance of the underwater domain and emerging threats require a new approach not only at national level but also a stronger awareness and cooperation among Allies[77]. Underwater security requires multinational-interagency cooperation and can only be achieved through working together with national, regional and global maritime security organizations as well as civilian agencies, industry and research centers.

[75] "Civiltà del mare. Geopolitica, strategia, interessi nel mondo subacqueo". www.civiltadellemacchine.it/

[76] About ISA – International Seabed Authority

[77] NATO and the protection of critical energy infrastructures - Nato Defense College Foundation (natofoundation.org)

For this reason, the Italian Navy is elaborating a proposal to offer the Alliance the establishment of a NATO Underwater COE (Centre of Excellence). Italy has a big potential in terms of geo-strategic position[78] since she is in the middle of Mediterranean Sea. Moreover, the presence of the NATO Centre for Maritime Research and Experimentation (CMRE) that organizes and conducts scientific research and technology development centered on the maritime domain with a focus on underwater topics, could represent an important opportunity of synergy between science and doctrine for the needs of the Alliance. In addition, in the same premises in La Spezia, Italy has established the national underwater hub for the collaboration among government, private sectors, industries and academia in order to boost the underwater technology development, adapting it to the needs of the Navy. This initiative represents an important opportunity to strengthen NATO's capabilities and expertise in the field of underwater warfare, technological research, and underwater capability development[79]. The creation of a dedicated COE focused on underwater operations should be the consequence of the awareness of the strategic relevance of this domain and the need to enhance NATO's effectiveness in this area. By consolidating knowledge, skills, and resources, the COE can contribute to the development of concepts, doctrines, and operational strategies that can enhance the Alliance's underwater warfare capabilities. The COE will likely serve as a hub for collaboration among NATO member states, fostering information sharing, research, and innovation in underwater technologies and tactics. It can facilitate the exchange of best practices, lessons learned, and the development of standardized procedures in underwater warfare. This collective effort can lead to increased interoperability and operational effectiveness among NATO forces. Furthermore, the establishment of the COE aligns with NATO's ongoing efforts to adapt to emerging security challenges and technological advancements. As underwater capabilities become more critical in modern warfare scenarios, investing in research and development in this field is crucial for maintaining a competitive edge. Overall, this initiative could support the Alliance's commitment to stay at the forefront of *technological advancements and maintain a credible deterrence posture, providing a platform for NATO to enhance its skills, know-how, and potential in underwater warfare, ultimately bolstering the Alliance's overall defense capabilities.*

VI. Conclusion

Advancing deep-sea operations capability and contributing to the protection of critical underwater infrastructure is a harsh task for Navies that is becoming essential to contribute to national security. Relevant investment in continuous research and development and a whole-of-Nation effort are required to deliver effective capabilities and to ensure a proper monitoring and protection of the underwater operating environment, first by acquiring a persistent and reliable Underwater Situational Awareness. The establishment of networks comprising fixed and mobile sensors plays a crucial role in reaching UWSA. These sensor networks enable proactive monitoring and intervention on critical underwater infrastructure, leading to safer

[78] G20 Digitale? L’Italia è l'hub naturale per la connettività sottomarina. Parla Ascani - Formiche.net

[79] NATO - News: NATO Secretary General engages industry on critical undersea infrastructure, 05-May.-2023

and more efficient operations in the challenging deep-sea environment.

In addition to advanced technology, the complexity of the underwater domain requires also a new collaborative approach especially taking in consideration that critical seabed infrastructure are mostly private owned. Therefore, it is necessary to establish deep cooperation and joint procedures between Navies and private companies.

Finally, it is necessary to update the current legal framework at national and international level in order to guarantee a safe access to underwater spaces and a proper safeguard of critical seabed infrastructure.

This article presents a view on the Italian Navy approach to the underwater domain, which includes the plan to propose the establishment of a NATO Underwater Centre of Excellence to improve the Alliance overall capabilities to safeguard its interests in this challenging new operational domain.

A SHORT NOTE ON THE LEGAL ASPECTS OF THE PROTECTION OF CRITICAL MARITIME INFRASTRUCTURE AND THE ROLE OF NATO

Dr. Sofia GALANI

I. Introduction

The aim of this short paper is to shed light on the importance of safeguarding critical maritime infrastructure (CMI), associated legal issues, and the role NATO can play in its protection.

II. What is meant by 'maritime critical infrastructure'?

So far, there has been no strict definition of what CMI is.[80] The EU, for example, defines critical infrastructure as an asset or system which is essential for the maintenance of vital societal functions.[81] When referring to CMI, we collectively refer to ships, ports, undersea cables and pipelines, offshore installations, wind farms and LNG terminals. Certainly, this is not an exhaustive list. At the same time, we may all agree that this infrastructure is critical as they all perform vital societal functions, but one may question how 'critical' some of these are. For example, over the recent years, when we talk about CMI, the first that comes to our mind is undersea cables, pipelines, and energy installations. What might be 'critical' changes over time for different reasons. For example, the protection of ships and ports gained significant attention after the 9/11 attacks when States realized both how vital they are for the global economy and how prone to terrorist attacks. On the other hand, the debate on the protection of undersea cables and energy installations has been accelerated by a sequence of events, such as the war in Ukraine, the Nord Stream incident, the energy crisis, and hybrid warfare.[82] It is well-known that States have been shifting their traditional warfare methods from open hostilities to low intensity attacks against critical to the enemy infrastructure.[83] The execution of such attacks has been facilitated by the advancement of technology. In the past, it was difficult even for States to reach great depths at sea. Nowadays, not only States but non-state actors have the technology needed to cause damage to undersea cables and pipelines.

III. Legal and Practical Challenges in Determining What Critical Maritime Infrastructure Is

Since there is no strict definition of CMI in international law, States can determine what CMI is in their domestic law. In doing so, States may take into consideration various criteria, such as the functions or financial importance of CMI, or the impact that a damage on CMI could have for the local population, the region, or

[80] Christian Bueger and Tobias Liebetrau, "Critical Maritime Infrastructure Protection: What's the Trouble?" (2023) *Marine Policy*, 2.

[81] https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en.

[82] Merlyn Thomas, "Nord Stream Blast Blew Away 50 Metres of Pipe", (18 October 2022) *BBC News*, https://www.bbc.com/news/world-europe-63297085.

[83] Arsalan Bilal, "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote" (30 November 2021) *NATO Review*, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and- trust-as-the-antidote/index.html

the international community. Arguably, deciding what classifies as CMI can be a political decision too.[84] But why is it important for States to determine in their domestic law what CMI is? The reason is that domestic law will enable them to design and implement national policies for the better protection of CMI as well as to designate the national agencies responsible for its protection. The lack of fixed criteria for determining CMI, however, results in inconsistent national policies that create significant challenges when CMI projects, such as pipelines, run across different States. In such cases, certain States will have more robust protection in place while others will not be able to meet these standards.[85]

IV. Who is Responsible for Protecting Maritime Critical Infrastructure and Under What Legal Basis

Threats to CMI include intentional threats, such as physical attacks, explosions, or interference with systems for collecting vital information for the security and defense of a State. These threats aim to harm State security, and this is why States are primarily responsible for protecting CMI. On the other hand, unintentional threats, such as vessel collisions, damage to underwater cables caused by a natural disaster, or normal "wear and tear" are usually dealt with by private entities in charge of installing, maintaining, and repairing CMI. In practice, however, this distinction between the responsibility of States and private entities can only be artificial and as will be later explained the cooperation of States and private actors is much needed to protect CMI.

For States to exercise jurisdiction over MIC, its location is essential to be determined. This happens as, apart from ships, CMI does not have a nationality and thus we need to examine what powers international law grants upon States in relation to its protection. A coastal State can exercise jurisdiction over CMI found within its territorial waters. Article 19 of the 1982 Law of the Sea Convention (LOSC) stipulates that the passage of a foreign vessel is not innocent if it engages in an 'any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State', giving the coastal State the right to suspend innocent passage or exercise criminal jurisdiction. The powers of a coastal State are more limited within its contiguous zone as it only exercises control to prevent and punish infringement of its customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea (article 33 LOSC). It is hard to see how sabotaging or damaging CMI would fit this provision unless such damage could perhaps affect the quality of water or be in breach of fiscal laws. Given the importance of natural and energy resources in the EEZ, coastal States are permitted to construct safety zones around artificial islands, installations, and structures (article 60 LOSC). The breadth of the safety zones cannot exceed a distance of 500 meters around them, but coastal States can exercise exclusive jurisdiction within this zone. This is noteworthy considering that it restricts the freedoms third States enjoy within the EEZ (article 58 LOSC), and particularly the freedom of navigation, emphasizing how pivotal it is for coastal States to safeguard CMI within their EEZ. Safety zones can also be designated around artificial islands, installations, and structures in the continental shelf

[84] Bueger and Liebetrau (2023), 1.

[85] Euronews, "Gemany and Norway Announce Plan to Better Protect Maritime Infrastructure (1 December 2022), https://www.euronews.com/2022/12/01/germany-and-norway-announce-plan-to-better-protect-maritime- infrastructure.

where article 60 applies *mutatis mutandis* (article 80 LOSC). The powers of States are not equally strong in the continental shelf regarding the protection of submarine cables and pipelines. Article 79 LOSC recognizes the right of all States to lay submarine cables and pipelines on the continental shelf and requires coastal States not to impede their laying or maintenance. According to the same provision, when laying submarine cables or pipelines, States shall have *due regard* to cables or pipelines already in position. The 'due regard' obligation, however, is not a strict one as it essentially requires States to give notice or engage in meaningful consultations with the coastal State, but States do not always pay attention to this obligation.[86] Things can become more complicated where overlapping claims exist. Under international law, States that are parties to a maritime delimitation dispute are not meant to exploit unilaterally natural resources and can only proceed to exploration and exploitation of natural resources if they reach a temporary agreement (articles 74 and 83 LOSC).[87] In addition, neither party to a dispute is allowed to proceed to exploration or exploitation of natural resources if these activities cause irreparable damage to the other party and if they do not compromise the final agreement.[88] With regards to security, CMI built in disputed areas will most likely not be effectively protected as it will be unclear which State can exercise jurisdiction, and conflicting jurisdiction can put such projects at further risk.

Besides LOSC, there are other treaties that could be relied upon for the protection of CMI. Article 2 of the 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf criminalizes the destruction of fixed platforms. Article 2 of the 1997 International Convention for the Suppression of Terrorist Bombings criminalizes the unlawful and intentional use of an explosive or other lethal device against an infrastructure facility with the intent to cause extensive destruction of such facility or where such destruction results in or is likely to result in major economic loss is an offence. Article 1 (2) defines an "infrastructure facility" as any publicly or private owned facility providing or distributing services for the benefit of the public, such as energy. It is clear, however, from the wording of the provision that it is applicable only in case a submarine cable or pipeline is destroyed because of a terrorist attack that involves explosives and there is no similar provision for the sabotage or destruction of submarine cables or pipelines by other terrorist means, such as by severing cables or tapping into them to intercept sensitive national security information.[89] With reference to ship and port security, the ISPS Code play a key role, subject to its effective implementation by shipping companies and port States.

[86] Sofia Galani, "Tensions and Cooperation in Realizing Maritime Security in the Mediterranean Sea: The Examples of Maritime Terrorism and Irregular Migration" (2022) *Italian Yearbook of International Law*, 105.

[87] See also the *Dispute concerning delimitation of the maritime boundary between Ghana and Côte d'Ivoire in the Atlantic Ocean (Ghana/Côte d'Ivoire)* ITLOS Judgment of 23 September 2017.

[88] Ibid. See also Maritime Delimitation in the Indian Ocean (Somalia v. Kenya), Preliminary Objections, Judgment, I.C.J. Reports 2017, p. 3.

[89] Galani (2022), 106.

V. The Role of NATO in Protecting Maritime Critical Infrastructure: What lies ahead?

The brief analysis of the existing legal framework for the protection of CMI demonstrated that it is mostly inadequate to respond to the constantly emerging threats against CMI. At the same time, it is highly unlikely that the risks to CMI will go away. It is thus urgent for NATO to start responding to these threats. The Nord Stream incident was a wake-up call for NATO. Since the incident, it has been more active to protect undersea infrastructure by conducting more patrols in the North Sea. In February 2023, NATO announced the creation of the new Critical Undersea Infrastructure Coordination Cell that "will enable better coordination between key military and civilian stakeholders and with industry, on an issue that is vital to our security".[90] This is an essential and very much needed step towards forging collaboration with NATO partners and the industry. As explained earlier, the industry holds vital, and often commercially sensitive, information about the development and maintenance of CMI. It is thus essential that NATO worked closer with private partners who will be able to share the know-how concerning the functions and vulnerabilities of these projects. It is also much needed to build a closer partnership with like-minded allies, such as the EU. NATO and the EU demonstrated their ability to build strong partnerships in the fields of security. Following their close collaboration in the fight against hybrid threats, they are now exploring options of a strong partnership in response to critical infrastructure.[91] Finally, NATO should invest in maritime capacity building. Enhancing NATO members' legal resilience is necessary to protect CMI. As discussed, without appropriate domestic laws that criminalize acts against CMI, it is difficult to punish the culprits. Legal resilience combined with state-of-the-art technology, such as unmanned systems, would enable NATO members to respond to threats to CMI more effectively.[92]

The continuous investment of States in CMI and their growing dependence upon it for absolutely essential daily tasks will only whet the appetite of their enemies as well as criminals to target CMI more viciously. It is therefore crucial for NATO and its allies to safeguard CMI and not only develop responsive mechanisms to the emerging threats, but also take robust proactive measures to protect CMI against willful attacks.

[90] https://www.nato.int/cps/en/natohq/news_211919.htm

[91] https://www.hybridcoe.fi/; Dick Zandee, Sico van der Meer, Adája Stoetman, "Countering Hybrid Threats: Steps for Improving EU-NATO Cooperation" (October 2021) Clingendael Report, https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf; EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure (29 June 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564.

[92] Njall Trausti Fridbertsson, "Protecting Critical Maritime Infrastructure – The Role of Technology" (6 April 2023), https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf.

LEGAL ASPECTS OF THE PROTECTION OF SUBMARINE COMMUNICATION CABLES: A PRIMER

Dr. Bleda KURTDARCAN

I. A world interconnected: The brief history of submarine communication cables

The world's first submarine communication cable was laid in 1850, linking Great Britain and France was. Less than a decade later in 1858, the first transatlantic cable connecting Ireland with Newfoundland became operational. In 1902 a cable linked the Philippines with California; thus, the entire world became interconnected.

The first transatlantic telephone cables went into service in 1956, and 32 years later, the first fiber optic cable connected Europe and America. Today a network of some 450+ submarine cable systems with more than 1300 landing points and covering over 1,3 million km constitutes one of the world's most indispensable infrastructure! These seabed cables transmit carry close to 99% of trans-oceanic data, voice, and video information between countries or continents by using fiber- optic technology.

As we rely increasingly on digital communication for business, financial and personal needs, the submarine cable network has become the backbone of the global economy. Thus, their vulnerability is the vulnerability of modern society. An interruption of the flow of data through submarine cables causes a loss of connectivity that may bring to a halt important military operations as well as government and commercial communications, in particular financial transactions. Breaking a single cable can leave millions without internet access and saddle companies with millions in losses.

II. Threats to undersea cables

Threats to undersea cables can be linked to either physical or network attacks. The fact that many of the cable management & control systems are linked to the internet because they are connected to remote operating centers across the world, makes them vulnerable to cyberattacks. On the other hand, physical damage to undersea cables has often been caused by accident, due to careless fishing or anchors of ships. However, both historically and recently, physical damage to cables has been intentional in nature as well. Today physical damage to cables can result from direct cutting, tapping, and targeting of landing sites.

III. Physical threats never been more real, stakes never been higher

With the growing dependance of the modern societies and governments on the information technologies and communication infrastructure, the world's oceans have become a target-rich environment that provides adversaries with incentives to develop undersea operational competence and strike these difficult-to-defend systems.

These cables are vulnerable to deliberate attack in many ways. The most basic method of attack is simply to break the cable. Their construction means that this task presents little difficulty either mechanically or through the use of small explosive charges. Finding these cables is equally simple. The location of the cables is widely promulgated in order to prevent accidental damage but there is little to stop adversaries from exploiting this information for nefarious ends.

Moreover, small submarines and unmanned underwater systems have become increasingly affordable and are no longer in the exclusive use of navies or other State agencies. They could, indeed, be used to deliver threatening payloads or to disrupt seabed infrastructure. At first glance, it may appear to be easier for malicious State and non-State actors to attack the landing point of submarine cables. However, there is a high probability of attacks from under the sea because detection is a rather difficult task (stealth), because they imply the advantages of surprise and of economy of force, and because they can circumvent defensive measures. A final incentive is the imposition of a cost-imposing strategy.

IV. 'Scant, antiquated, and no longer fit for purpose (?)': The International law governing submarine cables

Since the first cables were laid across the globe, little attention has been given to undersea cable protection. This lack of attention stems especially from the fact that private entities own the majority of the most important cables. This situation complicates efforts to institute time- and resource-intensive policies. In addition, a rather outdated and complicated law of the sea governs different parts of the sea, which presents barriers to implementing new policies.

a. 1884 Submarine Cables Convention

After the laying of the first transatlantic cable in 1866, States realized the value of submarine cables and the necessity for their protection against willful or culpably negligent interruption or obstruction in sea areas beyond their national jurisdiction. Consequently, in 1884, 30 States adopted the Convention for the Protection of Submarine Telegraph Cables (1884 Convention). It only regulates interference with telegraph cables, not with the freedom of laying them. Today, the Convention is in force for 41 States.

The treaty applies to all those cables which are outside the territorial waters of states and requires nations to incorporate the treaty provisions into domestic law. Its article 2 states that 'the breaking or injury of a submarine cables, done willfully or through culpable negligence…shall be a punishable offense. Article 10 is of the utmost importance for the right of States Parties to the Convention to stop and inspect (although in a most limited manner) foreign vessels suspected of having committed an offence and to collect (and transmit) evidence. This is a remarkable exception to the flag State principle(!).

That being said, the customary nature of this convention and therefore its relevance to contemporaneous problems is highly contested.

b.1958 Geneva Convention on the High Seas & Geneva Convention on the Continental Shelf

The 1958 Geneva Conference addressed submarine cables in two documents, namely, Convention on the High Seas (High Seas Convention) and the Convention on the Continental Shelf. Under the Conventions, the term 'submarine cables' applies not only to telegraph and telephone cables but also to high voltage power cables.

Article 27 of the High Seas Convention addresses damage to cables but fails to clearly prohibit the intentional damage to them. It leaves the persecutory powers on signatories, by stating that the party should 'take necessary legislative measures' to make breaking of cables a 'punishable offense.'

The rest of the articles on the matter (Articles 26(3), 27, 28 and 29) are almost identical with the respective rules already agreed upon in 1884. There is, however, a significant difference, insofar as the 1958 High Seas Convention does not explicitly provide for the right of warships and other State ships to identify the nationality of a merchant vessel suspected of having broken a submarine cable and to investigate the facts. Seemingly, enforcement of the rules on the protection of submarine cables has, thus, been reserved to the exclusive (criminal) jurisdiction of the flag State or the State of nationality.

c. 1982 UNCLOS

The provisions regarding submarine cables of the 1958 Geneva Conventions and some of the 1884 Convention have found their way into the 1982 LOSC.

Articles 113 to 115 of the UNCLOS are almost identical with Articles I, IV, and VII of the 1884 Convention. According to UNCLOS Article 58(2), these provisions are also applicable in the EEZ. In brief, the obligation to enact national legislation related to submarine cables is limited in two respects. First, the obligation to enact domestic criminal legislation applies to acts of breaking or injuring a submarine cable done willfully or through culpable negligence and to conducts calculated or likely to result in such breaking or injury'. Moreover, according to article 21, coastal states have the right (but not the obligation) to adopt regulations to protect submarine cables in their territorial waters.

Second, it only applies to flag States of culpable vessels, and to the States of nationality of those having broken or injured a cable and of the owners of submarine cables.

As is the case with the 1958 Conventions, Article 10 of the 1884 Convention on the right of the warships and other State ships of all States Parties to identify the nationality of a ship allegedly having broken a submarine cable and to establish the facts has not found its way into the UNCLOS.

The 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention), its Protocol and the 2005 amendments were not drafted with a view to also protecting submarine communications cable against terrorist attack.

Consequently, it is safe to say that while international law of the sea recognizes the right of all States to lay submarine cables, it seems to be almost silent on the question as to whether and to what extent such cables are subject to the jurisdiction of the States that own them or whose nationals have laid and operate them. In particular, it is doubtful whether they are entitled to take the measures necessary to protect them against malicious interference.

V. Main takeaways

- UNCLOS Article 113 does not make it clear which other States - other than flag State and state of the nationality of the perpetrator - also have jurisdiction over the breaking or injury to submarine cables beyond the territorial sea. However, it is also possible to argue that States having laid submarine communications cables, or whose nationals have laid and/or operate them, retain the right to exercise their jurisdiction in accordance with the well-established principles of international law, i.e., under the passive nationality and protective principle.

- Apart from international responsibility of the States for acts attributable to them, the only remedies available in cases of interference with submarine cables are either the right of self- defense or responsibility 'for shirking "jurisdictional control" over ships flying its flag in respect of "administrative, technical and social matters."

- With regard to the right of self-defense, whether attacks on submarine cables on the continental shelf and the EEZ as well as on the high seas, would constitute 'the most grave form' of use of force qualifying as an 'armed attack' against a particular State (or States) is not straightforward. A quantitative ('scale') and qualitative ('effects') argument face significant limitations. The main challenge is that it is unclear against which State an alleged 'armed attack' takes place.

- The undersea cable network is part of a very complex set-up of diverse public and private actors operating, regulating and protecting the infrastructure, which straddles different policy fields, including territorial sovereignty, maritime security, cyber security, digital, infrastructure, telecommunications, fishery, shipping, and marine environment protection. Its legal regime is therefore, far from complete, coherent, and up to date.

CYBER THREAT INTELLIGENCE: MITIGATING RISKS TO MARITIME SECURITY

Emre Halisdemir*, Jacob Galbreath, Vasco Prates, Sungbaek Cho

Cooperative Cyber Defence Centre of Excellence (CCDCOE)*(Emre.Halisdemir@ccdcoe.org)

I. Introduction

Sustaining and enabling human activity, the Sea has an overall fundamental role in world economy and human development. In fact, on Earth, it is one of the most important providers of natural resources and renewable energies, but also an enabler of the transportation of goods, people, energy and data, bridging this way the human activity. Overall, the Sea has become an essential environment to boost human economy and sustainability. This pronouncement also discloses a persistent and exponential increase of commercial exchanges between Nations, and proportionally in an increase in the number of vessels, land-sea interfaces, underwater cables and pipelines, just to name a few. Associated to this increase of human activity and pursuing optimization and productivity goals to foster Maritime growth, technology takes on an ever- growing role in the management of systems and equipment, but also to exchange information between people, those same systems, and equipment. All to provide faster, precise and better command and control solutions for overall activities and actions in the Maritime environment. Technologies are implemented, infused, layered, and stacked in the Maritime environment with clear aims to promote better and faster Maritime growth and safety.

Modern technologies, described as Information technology (IT) and operational technology (OT), in this high evolving environment, have become essential in order to communicate and interface actions or activities with intended and consistent effects, revealing its increasing importance, role, and proportion of the Maritime environment. The complexity of the larger Maritime ecosystem gets even bigger when IT and OT interconnects and expands to the broader Internet as well as to its alias controllers or users, extending this way, the Maritime environment to cyberspace.

Besides new opportunities and challenges, new risks arise upon the Maritime environment, beyond “traditional” and already recognized risks associated in other environments. These risks, brought by cyberspace into the Maritime environment may magnify into perfect storms, for which we must be prepared for, avoid, or mitigate. Maritime cyber risk is already recognized by the International Maritime Organization (IMO) which refers to it as; a measure of the extent to which a technology asset could be 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[93]. This consequential effect could be a result of an action or act initiated in or through cyberspace to cause harmful effects, i.e.

[93] Maritime Cyber Risk, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (Accessed on 8/5/2023)

cyberattack[94]. The harmful effects infused on the Maritime environment, e.g. ports, terminals, ships or vessels, could imply shutting down of operations, creating port paralysis, cause environmental disaster even human injuries or death[95]

.

This projection results in the obvious need to identify and address technology weaknesses and vulnerabilities. IT systems, OT systems, as well as the information pertaining within those systems, must be protected against current and future threats. When IT or OT system threats are identified, we then are able to assess the risk upon those associated activities or actions. Protection should be aimed to entities in the Maritime environment, such as vessels, ports, and other maritime infrastructure. Additionally, we should also take into consideration the associated supply chain when addressing Maritime cyber risks. To manage cyber risks effectively (i.e., accept, mitigate, avoid or transfer) identification and situational awareness of cyberspace threats is essential, with a special focus on those that could harm the Maritime sector. Cyber threats are defined as any circumstance or event with the potential to adversely impact operations, assets, individuals, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, or denial of service[96]. Therefore, it is clear that the maritime sector presents a high cyber risk, which demands, in its assessment, a proper knowledge of the man-made things in the maritime environment. A proper awareness to tackle the risks requires a comprehensive approach to the environment attack surface and to the cyber threat landscape.

While cybersecurity improvements are already in place in sectors such as energy, banking, and communications, the maritime sector still lacks behind. Furthermore, considering that in cyberspace, borders between countries, public and private entities, are blurred, a timely identification of cyber threats is of paramount importance to identify, monitor, trace, and act. Therefore, it is crucial to address cybersecurity in the maritime environment through structured processes like common and timely identification and sharing cyber threats.

II.Cyber Incidents in the Maritime Sector

Circumstances and events in the Maritime environment contain specificities unique to the cyber ecosystem. Examples of these unique systems and its components[97] would include terminal access control systems, terminal operating centre's systems, cargo handling and management systems, vessel traffic monitoring and control systems, shipping companies' enterprise systems, shipboard and onshore IT/OT systems which make

[94] Accordingly with "The Official NATO Terminology Database, available in https://nso.nato.int/natoterm/Web.mvc

[95] Additional effects detailed in European Union Agency for Cybersecurity (ENISA), Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector, 26 November 2019, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime- sector.

[96] Cyber Threat, https://csrc.nist.gov/glossary/term/cyber_threat (Accessed on 8 May 2023)

[97] U.S. Department of Transportation, ICS Security in Maritime Transportation: A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure, July 2013, https://rosap.ntl.bts.gov/view/dot/10057

attractive targets for malicious actors, state and non-state actors. Technology and its application on all of the above examples, require a broader scale consideration when involving the considerable amount of data to be prepared and exchanged between ships and ports. Ships need to digitally interact with shore-based operations and service providers. This digital interaction includes sending dozens of different documents via email, online portals, or other communications means[98]. Malicious actors would be typically interested in exploiting these data as a logical and apparent attack vector. Other recognized vectors could be the amount and variety of OT systems/components in the Maritime sector that, due to the life spam of ships, could be or become insecure for being outdated/deprecated or lacking on time or consistent patching. In general, OT systems have a considerable number of weaknesses when compared to IT systems[99]. Since OT system often have a lifespan of 10 years or more, many components are past end of life technical support. These OT components may not be supported or be compatible with state-of-art cybersecurity technologies. Even if security patches are available, applying them is generally not easy, as it often requires significant disruption to operations. OT systems have limited computing power and memory, making it difficult to implement feature-rich security functionalities. Whereas vendors of OT systems tend to have not considered security as an essential part of development process during production, implementation is slow when compared to IT products, despite developer awareness and global concerns about security. Additionally, communication protocols used in OT systems generally lack sufficient authentication or encryption methods, and are therefore vulnerable to disruption or manipulation attacks, causing failure of command-and-control processes[100]. Moreover, modern OT systems are even more interconnected with IT systems for business/operational efficiency. According to a survey of 338 organizations (not specific to the maritime sector) in 2019[101], only 28% were operating OT systems in isolated environments with no external connections. Like other sectors, the use of wireless sensors and wireless networks is also increasing, where the maritime sector is not an exception, e.g. smart ports initiatives. Smart ports are ports that autonomously process port operations and optimize logistics flow by applying new and advanced technologies to automate and process real time operations, a significant number of initiatives around the globe are already in place, like in US (Savannah, Houston, Los Angeles), Germany (Hamburg), the Netherlands (Rotterdam), Singapore (TUAS), Korea (Incheon) and so on[102]. Most of them use wireless technologies, which could be exploited by attackers when wireless equipment/devices are not properly configured and provisioned (e.g., the use of authentication/encryption mechanisms, improper storage

[98] Aviv Grafi, Why Ports Are at Risk of Cyberattacks, Dark Reading, 9 September 2022, https://www.darkreading.com/attacks-breaches/why-ports-are-at-risk-of-cyberattacks

[99] U.S. Department of Homeland Security (DHS) (2016), Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 2016, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[100] Eric Knapp and Joel Langill (2015), Industrial Network Security, 2nd Edition, ISBN: 9780124201149, Syngress, 2015

[101] Barbara Filkins (2019), SANS 2019 State of OT/ICS Cybersecurity Survey, SANS Institute, June 2019, https://www.sans.org/reading-room/whitepapers/analyst/membership/38995.

[102] UN The Economic and Social Commission for Asia and the Pacific (ESCAP), Smart Ports Development Polices in Asia and the Pacific, February 2021, https://www.unescap.org/sites/default/d8files/event-documents/SmartPortDevelopment_Feb2021.pdf.

of shared sensitive information or by the installation of backdoors into the devices during a provisioning process). Moreover, wireless signals can be prone to radio frequency jamming attacks and spoofing as well as hijacking of signals can be possible if there is any error in the design or implementation of wireless protocols.

There have been a number of publicly disclosed incidents in the maritime sector due to the lack of cybersecurity (summarized in Table 1). All of the attacks initially targeted IT systems of shipping companies and ports/terminals, and with some attacks causing disruption to cargo loading/unloading operations as well. Maersk, a Danish container shipping company, became victim of NotPetya in 2017, which seized control of the software update mechanism of M.E.Doc, the de facto standard accountancy package for companies doing business in Ukraine. In Maersk's case, no customer or business data was believed to have been exposed. However, the company experienced severe disruptions which forced it to halt operations for 10 days as the ransomware spread through core IT systems, while ships with 10 to 20 thousand containers were entering a port every 15 minutes. In total, Maersk reinstalled 4,000 servers, 45,000 PCs, and 2,500 applications. The company projected that this cyberattack cost up to $300 million in lost revenue[103].

Date	**Cyber Incident**
June 2021[104]	A South Korean container shipping company, HMM, stated that the unidentified cybersecurity breach was detected, which led to limited access to the company's Outlook email system in certain regions.
July 2021[105]	A Japanese container shipping company, Kawasaki Kisen Kaisha, confirmed that its computer systems had been breached with unauthorized access to overseas subsidiary systems just after its leaked data had been published. In March 2021, the company's enterprise system was disrupted due to a cyberattack and it took several weeks to fully restore the system.
July 2021[106]	A major port operator in South Africa, Transnet, was hit by a cyberattack, which has disrupted container operations. Cargo handling at container terminals of four major ports were affected, causing backlogs and hampering export until the system restoration.

[103] Charlie Osborne, "NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs," ZDNET, 26 January 2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/.

[104] Antonia Din, South Korean Company HMM Reveals It Had Suffered a Cyberattack on Its Email Servers, Heimdal, 17 June 2021, https://heimdalsecurity.com/blog/hmm-reveals-it-had-suffered-a-cyberattack-on-its-email- servers/

[105] Japan's "K" Line Apologizes for Second Cyberattack in Months, ZDNET, 2 July 2021, The Maritime Executive, https://www.maritime-executive.com/article/japan-s-k-line-apologizes-for-second-cyberattack-in-months.

[106] Zandi Shabalala and Tanisha Heiberg, Cyberattack disrupts major South African port operations, 22 July 2021, https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/

September 2021[107]	A French container shipping company, CMA CGM, exposed its customer data due to a cyberattack but the attack did not cause the disruption of any critical systems.
November 2021[108]	A South Korean commercial and military shipbuilder, Daewoo Shipbuilding & Marine Engineering stated that there were hacking attempts on the company's networks. There was another attempt in June 2021 and it is unknown to the public if the attack was successful.
November 2021[109]	A Singapore-based shipping company, Swire Pacific Offshore, suffered from data breach of due to unauthorized access to their systems. The leaked data included some confidential proprietary commercial information as well as personal data.
August2021[110]	The Port of Houston in the U.S. issued a statement saying it had successfully defendedagainst an attempted hacking and no operational data or systems were impacted. CISAsaid that it believed a state actor was behind the hack.
February2022[111]	Cyberattacks happened to multiple oil port terminals in Belgium, Netherlands and Germany causing a disruption of IT services and/or affecting loading/unloading operations. An energy company, Shell, was forced to reroute supplies to other depotsbecause of the attacks to Germany.
February2022[112]	The Jawaharlal Nehru Port Container Terminal in India was hit by a cyberattack, which disrupted the terminal's management information system. The terminal had todivert one of its scheduled vessels to the nearby terminal.
December2022[113]	The Port of Lisbon in Portugal had been targeted by ransomware attack. Incident didnot compromise operational activity but its website went down. LockBit ransomwaregroup claimed that they have stolen financial reports, contracts, ship logs and other information about cargo and crews.

[107] CMA CGM reports another cyberattack targeting customer data, Ship Technology, 21 September 2021 https://www.ship-technology.com/news/cma-cgm-reports-another-cyberattack/.

[108] Shipbuilder confirms new possible cyberattack, Safety4Sea, 2 November 2021, https://safety4sea.com/shipbuilder-confirms-new-possible-cyber-attack/

[109] Jessica Haworth, Maritime giant Swire Pacific Offshore suffers data breach following cyber-attack, The Daily Swig, 26 November 2021, https://portswigger.net/daily-swig/maritime-giant-swire-pacific-offshore-suffers-data- breach-following-cyber-attack.

[110] Alan Suderman, Port of Houston target of suspected nation-state hack, AP News, 24 September 2021, https://apnews.com/article/business-technology-rob-portman-1e9ff8dac8dbb500d15661c816c22084.

[111] Jonathan Greig, Prosecutors investigating cyberattacks affecting multiple Belgian and Dutch ports, ZDNET, 3February 2022, https://www.zdnet.com/article/cyberattack-affecting-belgian-port-operations/

[112] Angelo Mathais, Ransomware attack hits Nhava Sheva container terminal, 22 February 2022https://theloadstar.com/ransomware-attack-hits-nhava-sheva-container-terminal/.

[113] Jonathan Greig, Port of Lisbon website still down as LockBit gang claims cyberattack, The Record, 29 December 2022, https://therecord.media/port-of-lisbon-website-still-down-as-lockbit-gang-claims-cyberattack.

January2023[114]	A Norwegian maritime organization, DNV, was hit by ransomware attack, which caused shut down of the IT servers connected to their Ship Manager system (vessel management supporting system) and around 1000 vessels were affected.
March 2023[115]	A Dutch maritime logistics company, Royal Dirkzwager, has confirmed that it was hitwith ransomware from the Play group. The attack did not have an effect on operationsbut did involve the theft of data from servers that held a range of contracts and personalinformation.
April 2023[116]	A German superyacht and military shipbuilder, Lürssen, was hit by a cyberattack,which has brought large parts of the company's shipyard operations to a standstill.
April 2023[117]	A US commercial and military shipbuilder, Fincantieri Marinette Marine was hit by acyberattack, which targeted servers that held data used to feed instructions to the shipyard's computer numerical control manufacturing machines and caused them offline for several days.

Table 1. Some Recent Examples of Incidents in the Maritime Sector

One thing to note is that there have been no reported cases of direct attacks on OT (such as shipboard systems or port facilities systems) as of yet. However, researchers at University of Plymouth in the UK demonstrated how supply-chain and controller device firmware attacks could compromise a large container ship's rudder[118]. Moreover, according to a survey of 125 senior US port and maritime terminal executives, respondents had the biggest concern in vulnerabilities of OT systems and they answered that OT systems were the fourth most frequent cause involved in actual data breaches[119].

Jamming Global Positioning System (GPS)/Global Navigation Satellite System (GNSS) signals by sending out more powerful signals has been one of the greatest concerns in the maritime sector for years. There have been a number of GPS/GNSS jamming incidents around the globe, including Mediterranean Sea, Persian Gulf,

[114] Jonathan Greig, Ransomware attack on maritime software impacts 1,000 ships, The Record, 17 January 2023, https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships.

[115] Jonathan Greig, Dutch shipping giant Royal Dirkzwager confirms Play ransomware attack, The Record, 17 March 2023, https://therecord.media/royal-dirkzwager-ransomware-attack-dutch-shipping.

[116] Phil Muncaster, Superyacht-Maker Hit by Easter Ransomware Attack, Infosecurity Magazine, 13 April 2023, https://www.infosecurity-magazine.com/news/superyachtmaker-easter-ransomware/.

[117] Sam LaGrone and Mallory Shelbourne, Ransomware Attack Hits Marinette Marine Shipyard, Results in Short-Term Delay of Frigate, Freedom LCS Construction, USNI News, 20 April 2023, https://news.usni.org/2023/04/20/ransomware-attack-hits-marinette-marine-shipyard-results-in-short-term-delay-of-frigate-freedom-lcs-construction.

[118] Kimberly Tam, Rory Hopcraft, Kemedi Moara-Nkwe, Juan Palbar Misas, Wesley Andrews, Avanthika Vineetha Harish, Pablo Giménez, Tom Crichton, Kevin Jones (2022), Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety, Journal of Transportation Technologies, Vol.12 No.1, DOI: 10.4236/jtts.2022.121001

[119] Jones Walker LLP. (2022), 2022 Ports and Terminals Cybersecurity Survey, https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey- Report.html

and the Red Sea in 2022[120], which resulted in lost or inaccurate GPS/GNSS signals affecting bridge navigation, GPS/GNSS-based timing, and communications equipment. GPS/GNSSspoofing is about sending a fake signal to cause drivers, ship captains and other operators to go off course.The spoofing can also affect operations that rely on accurate clock information. In 2013, the University ofTexas demonstrated a yacht hijacking with GPS spoofing, which was just one year after since they had demonstrated a drone hijacking in 2012. More recently, there was a hijacking demonstration of the Tesla Model 3's Navigate on Autopilot (NOA) system by an Israeli cybersecurity company[121]. Military-grade GPS/GNSS signals are protected by encryption against manipulation but signals used for commercial applications are not encrypted, and therefore manipulation can remain undetected. Although attacks on GPS/GNSS signals can affect the security of the maritime sector, experts often regard them as electronic warfare (EW) instead of cybersecurity. Likewise, issues related with fraudulent use of Automatic Identification System (AIS) can also be viewed as the outside scope of cybersecurity. Although AIS is regarded as one of main sources of maritime situational awareness and traffic monitoring, it suffers from aproblem of trustworthiness of messages because a shutdown or misinformation about the vessel's current status is possible by malicious intentions of ship operators[122]. There have been a number of misuses of AISaround the globe for years. For example, in 2022, a Russian oil tanker broadcasted false positions via its AIS transponder to circumvent sanctions[123]. Besides the risks of fraudulent uses of AIS by human, the VHFradio communications channel used by AIS can also be spoofed and hijacked[124] and there are several technical countermeasures against spoofed AIS messages, such as determining the validity of a message against legitimate historical messages[125] and using the radar sensor as a complement[126].

III.Cybersecurity Measures in Maritime Sector

Nations and international organizations consider the importance of maritime cybersecurity to be crucial, designating it as critical national infrastructure (CNI) or critical information infrastructure (CII)[127] and put significant efforts to keep it secure.

It has not been very long since IMO officially recognised the importance of cybersecurity. In 2016, IMO issued a temporary risk management guideline (MSC.1/Circ.1526) for the shipping industry, which was

[120] U.S. Department of Transportation, MSCI Advisory: 2022-010-Various-GPS Interference & AIS Spoofing, 9September 2022, https://maritime.dot.gov/msci/2022-010-various-gps-interference-ais-spoofing.

[121] Roi Mit, 'Top 10 GPS Spoofing Events in History,' Threat Technology, https://threat.technology/top-10-gps-spoofing-events-in-history, (Accessed 8 May 2023).

[122] Cyril Ray, Clément Iphar, Aldo Napoli, Romain Gallen and Alain Bouju, 'DeAIS Project: Detection of AIS Spoofingand Resulting Risks,' OCEANS 2015, pp. 1-6, 2015, doi: 10.1109/OCEANS-Genova.2015.7271729.

[123] Chris Cook, David Sheppard and Polina Ivanova, How a Russian oil tanker tried to conceal its location, FinancialTimes, 7 December 2022, https://www.ft.com/content/90dcc9b7-3371-411e-9d80-a2be0b4c10ca.

[124] Marco Balduzzi, Kyle Wilhoit and Alessandro Pasta, 'A Security Evaluation of AIS,' Trend Micro, 2014, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation- of-ais.pdf

[125] Ray et al., 'DeAIS Project: Detection of AIS Spoofing and Resulting Risks.'

[126] Fotios Katsilieris, Paolo Braca and Stefano Coraluppi, 'Detection of Malicious AIS Position Spoofing by Exploiting Radar Information,' The 16th International Conference on Information Fusion, pp. 1196-1203, 2013.

[127] CII is a terminology that stresses the importance of cybersecurity as opposed to conventional critical (national)infrastructure.

superseded by a formal guideline MSC-FAL.1/Circ.3[128] the next year. In 2017, IMO adopted Resolution MSC-428(98)[129], requiring member states to apply a cybersecurity risk management approach to the safety management systems of ships. Although these documents only provided very high-level principles, they can be regarded as a significant step towards cybersecurity in the marine sector.

In Europe, EU Directive 2016/1148 on the security of network and information systems (NIS Directive)[130] and its revision Directive 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive)[131] include the maritime sector as a part of the bigger "transport" sector in their scope. These Directives define the EU's minimum rules for a regulatory framework to increase cybersecurity andresilience in both public and private organizations. The Directives identify maritime operators, including passenger and freight water transport companies, and the managing bodies of ports and operators of vesseltraffic services as 'Operators of Essential Services' (OES) and impose stricter cybersecurity requirements. European Union Agency for Cybersecurity (ENISA) has also published several cybersecurity reports and guidelines in regards to maritime security. In 2011, ENISA published the first EU report on cybersecurity challenges in the maritime sector[132] to raise cybersecurity awareness. In 2019, ENISA published a "Good Practices" guideline[133] for port authorities and terminal operators with a list of potential threats and securityrecommendations and, in 2020, it also published a detailed risk management guideline for port[134].

Large parts of systems used in ports and ships can be regarded as specialized implementations of generalIT and OT systems. Therefore, cyber threats appearing in other critical infrastructure sectors are equally applicable to the marine sector. There are a number of general cybersecurity guidelines with a list of threatsand corresponding security measures, including international cybersecurity management standards such as ISO/IEC 27001[135], ENISA's cyber hygiene practices[136] and US CISA's cybersecurity essentials[137]. There are

[128] MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management,' International Maritime Organization, 4 July 2017, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[129] Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems,' International Maritime Organization, 16 June 2017, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[130] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures fora High Common Level of Security of Network and Information Systems across the Union, 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.

[131] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures fora high common level of cybersecurity across the Union, 14 December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

[132] European Union Agency for Cybersecurity (ENISA), Cyber Security Aspects in the Maritime Sector, 19 December 2011, https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

[133] ENISA), Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector.

[134] European Union Agency for Cybersecurity (ENISA), Guidelines - Cyber Risk Management for Ports, 17 December 2020, https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.

[135] Standardization (ISO) (2013), ISO/IEC 27001:2013: Information technology -Security techniques - Information security management systems - Requirements, 2013, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed- 2:v1:en.

[136] European Union Agency for Cybersecurity (ENISA), *Review of Cyber Hygiene practices* (December 2016), https://www.enisa.europa.eu/publications/cyber-hygiene/@@download/fullReport

[137] U.S. Cybersecurity & Infrastructure Security Agency (CISA), *Cyber Essential Starter Kit* (2021), https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0. pdf.

also a number of guidelines for general OT systems cybersecurity, including US DHS's Recommended Practice[138], US NIST's Special Publication 800-82[139] and German BSI's Top10 Threats and Countermeasures[140]. These standards, best practices and guidelines can be used as excellent references when starting to improve the maritime cybersecurity.

Regarding the maritime sector by itself, only a few references exist at present. The ENISA's guideline published in 2020[141] is one of the most extensive work dedicated to port cybersecurity. As for cybersecurityof ship on-board systems, the Baltic and International Maritime Council (BIMCO) published a detailed guideline in 2016, of which the latest version was published in 2020[142]. UK Department for Transport also published the "Code of Practice for Cyber Security for Ships,"[143] which is similar to the BIMCO guideline.In 2022, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) published a report on cybersecurity threats and security measures for autonomous ships[144].

However, no matter how stringently cybersecurity measures are applied, cyber incidents cannot be completely prevented. Attackers, especially state (sponsored) hackers, persistently study how to infiltrate the system and continue to develop new tactics, techniques and procedures (TTPs). Moreover, attackers areactively exploiting n-day vulnerabilities, which are exploited on the same day or within a very short time period after vulnerability disclosure.

According to a security company's analysis[145], the number of vulnerabilities found in OT systems is increasing annually from 550 vulnerabilities in 2020, through 1,191 in 2021, to 1,342 in 2022. However, even if they are deployed in a timely manner, security patches for OT systems are not easy to apply since it usually requires systems to stop operations of facilities. Applying patches needs to be planned and notifiedseveral weeks in advance to minimize business impact and confusion. In addition, these patches need to bethoroughly tested to check potential incompatibility problems with existing systems and components, whichtakes a tremendous amount of time. In order to overcome these limitations, it is essential to obtain information and TTPs on attacks as quickly as possible and identify and apply immediately applicable measures to prevent/minimize

[138] U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* (September 2016), 16-20, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[139] U.S. National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security*, NISTSpecial Publication 800-82 Revision 2 (May 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf..

[140] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Industrial Control System Security Top 10 Threats and Countermeasures, v1.3* (June 6, 2019), https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf.

[141] ENISA, Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector

[142] The Guidelines on Cyber Security Onboard Ships - Version 4,' Baltic and International Maritime Council, 23 December 2020, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[143] Code of Practice: Cyber Security for Ships,' UK Department for Transport, 13 September 2017, https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice.

[144] Sungbaek Cho, Erwin Orye, Gabor Visky and Vasco Prates, Cybersecurity Considerations in Autonomous Ships,CCDCOE, August 2022, https://ccdcoe.org/library/publications/cybersecurity-considerations-in-autonomous- ships.

[145] SynSaber, Industrial CVE Retrospective, February 2023, https://synsaber.com/resources/datasheets/ics-cve-reports/industrial-cve-retrospective-2020-2021-2022/.

incidents. In this sense, it is quite important to share threat information/intelligence between relevant organisations.

IV. Cyber Threat Intelligence

According to US NIST SP800-15[146], cyber threat information is defined as any information that can helpan organization identify, assess, monitor, and respond to cyber threats. Typical examples of cyber threat information are Indicators of Compromise (IoC), Tactics, Techniques and Procedures (TTPs), security alerts, threat intelligence reports and security tool configurations, as summarized in Table 2. These examples provide information necessary for organizations to deal with cyberattacks from technical perspectives. However, a broader concept of cyber threat information includes any kind of information thatcan be useful for an organization to prepare against cyberattacks and increase the level of security posture.This view of cyber threat information may include cybersecurity best practices (methods for organizing, securing and maintaining systems/networks) and attribution (identifying who is responsible for specific malicious activities)[147].

Type	**Description**
Indicators of compromise (IoCs)	IoC are technical artifacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control (C2) server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.
Tactics, techniques andprocedures (TTPs)	TTPs describe the behaviour of an actor. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique.
Security alerts	Security alerts known as advisories, bulletins, and vulnerability notes, are brief, usually human readable, technical notifications regarding current vulnerabilities, exploits, and other security issues.

[146] U.S. National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing,* NIST Special Publication 800-150 (October 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[147] Michael Daniel and Joshua Kenway, Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO, Proceedings of the 12th International Conference on Cyber Conflict(CyCon), T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.), NATO CCDCOE, pp 179-193, https://ccdcoe.org/uploads/2020/12/9-Repairing-the-Foundation_ebook.pdf

Threat intelligence reports	Threat intelligence reports are generally prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organization. Threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes.
Security tool configurations	Tool configurations are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. Tool configuration information could consist of instructions on how to install and use a malware removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

Table 2. Examples of Cyber Threat Information (Source: NIST P800-50)

These days, a number of government entities and private cybersecurity/IT companies use the term "cyber threat intelligence" (CTI in short) instead of "cyber threat information." While cyber threat information is a more general terminology that was widely used in the past, cyber threat intelligence could be regarded asa means to address analytic, interpretive, predictive and proactive aspects of cyber threat information. Although there is certain distinction between "intelligence" and "information"[148], both words in practice (and subsequently, in this paper) are used interchangeably.

Sharing of cyber threat information ("information sharing" in short) provides an organization access to information that might otherwise be unavailable to it, enabling so-called collective cyber defence. A typical example structure to facilitate information sharing is a trusted forum or platform where critical infrastructure owners or operators can have face-to-face discussion; frequently (but not exclusively), such groups are moderated or facilitated by a public sector agent[149]. The forum may utilize an online bulletin board system allowing the forum members to have access to it from the internet. An advanced system mayalso be used to automatically reflect received IoCs to security tool configurations. There are a number of benefits of information sharing, including[150]:

- Shared Situational Awareness. Information sharing enables organizations to leverage thecollective knowledge, experience, and analytic capabilities of their sharing partners;
- Improved Security Posture. Using shared information, organizations can identify affected

[148] Intelligence, by the definition of NATO, is the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threatsand offer opportunities for exploitation by decision-makers. See: https://nso.nato.int/natoterm/content/nato/pages/home.html

[149] European Union Agency for Cybersecurity (ENISA), *Incentives and Challenges for Information Sharing in theContext of Network and Information Security*, 8 September 2010, https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing/@@download/fullReport.

[150] U.S. National Institute of Standards and Technology, *Guide to Cyber Threat Information Sharing,* NIST SpecialPublication 800-150

platforms or systems, implement protective measures, enhance detection capabilities, and moreeffectively respond and recover from incidents based on observed changes in the threatenvironment. As organizations share information and subsequently mitigate threats, they can improve their overall cybersecurity posture;

- Knowledge Maturation. When seemingly unrelated observations are shared and analysed by organizations, those observations can be correlated with data collected by others;
- Greater Defensive Agility. Actors continually adapt their TTPs to try to evade detection, circumvent security controls, and exploit new vulnerabilities. Organizations that share information are often better informed about changing TTPs and the need to rapidly detect and respond to threats.

While these benefits are directly related to improvement in situational awareness and cybersecurity posture, there are also a number of benefits from economic and psychological perspectives. According to ENISA's research in 2010[151], cybersecurity experts rated the efficient allocation of cybersecurity resourcesand cost savings as the most important incentive from information sharing, and the incentive stemming from the quality, value and use of information shared as second to the cost savings. Despite these potentialbenefits, it seems that information sharing in practice is not highly regarded amongst institutions. Organizations in both the public and private sectors fear losing reputation and trust by the public disclosureof cyber security breaches. Moreover, incident information from a specific company might provide its competitors opportunities to take commercial advantages[152]. There are two main ways to strengthen the private sector's participation in information sharing. One is to mandate it by laws and the other is to provideexplicit incentives (other than the benefits mentioned above) to companies actively participating in information sharing. Mandating information sharing by laws has usually limited scope in terms of target organizations and contents to be shared since mandating "all" companies to report "all" information wouldbe excessive regulation. Current legal practices require only critical infrastructure operators to "promptly"report to the government and share related IoCs in the event of a significant incident, and these practices have only recently begun to operate effectively. Provision of visible incentives (e.g., tax reduction, endowing a preferred contractor status for government procurement, etc.) could motivate companies to participate more actively in information sharing. However, it is not easy to establish criteria about what kind of incentives to give for information sharing activities at differing levels; in particular, the idea that only big companies with large cyber security departments would reap the majority of these incentives is bound to cause controversy. Beyond these two methods, the primary way to expand information sharing inthe private sector is to encourage voluntary participation by making companies perceive the real value of the practice. One such action that would underscore this value for private companies is for the governmentto actively provide feedback (such as investigation results and relevant

[151] ENISA, *Incentives and Challenges for Information Sharing in the Context of Network and Information Security*

[152] For this concern, the NIS2 Directive requires that the information exchanged must be limited to that which is relevant and proportionate to the purpose of that exchange and the exchange of information must preserve the confidentiality of that information and protect the security and commercial interests of entities concerned

information) so that companies know the information sharing is not unidirectional and benefits both sides. Reciprocal and continuous exchange of information is a key for success in information sharing. The government should establish a formal security review and anonymization process, to be performed on either the government or the company side or on both, for companies to dispel concerns about leakage of sensitive or personal information.

Law enforcement and security/intelligence/defence agencies may also be reluctant to share their information. There have been some legal provisions to allow those agencies to share confidential/classified information with other public and private organizations. For example, US Cybersecurity Information Sharing Act of 2015[153] allows federal agencies to produce declassified information and share it with relevant parties at an unclassified level. In the past, the sharing of governmental information to the private sector was the exception to the rule, since unauthorized disclosure of the intelligence by other parties could causenegative impacts on, and in the worst case jeopardize, on-going investigation, monitoring/tracing and otherlawful activities. For example, NSA Cybersecurity Directorate Director Rob Joyce said that it was "in ourDNA" to protect sources and methods to ensure the ability to "know secrets into the future" when he gavea public speech on the importance of information sharing between public and private sectors last year. However, he said "what we know is often not sensitive, it is how we know it" and "we can make availablethe insights about what we know without putting at risk how we know it."[154] In order to strengthen information sharing from the government to the private sector, the government agencies must be aware of the fact that the more they provide information to the private sector the more they would receive informationin return. Explicitly requiring the government agencies to share information with the private sector by national cybersecurity strategy or other regulations/directives would be helpful to strengthen such information sharing. For example, the new US national cybersecurity strategy[155] announced in March 2023emphasizes the importance of information sharing. The strategy states that operational collaboration modelsat Sector Risk Management Agencies (SRMAs)[156] would provide opportunities to enable timely, actionable,and relevant information sharing directly with private sector partners in their respective sectors, while designating CISA as the national coordinator for SRMAs to enable the US Government to scale its coordination with critical infrastructure operators across the country. The NIS2 Directive also addresses theimportance of information sharing with the private sector. Although it

[153] US Congress, Cybersecurity Information Sharing Act of 2015, PUBLIC LAW 114–113—DEC. 18, 2015, 18, December 2015, Pages 696 – 716, https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

[154] Christian Vasquez, "NSA cyber chief says Ukraine war is compelling more intelligence sharing with industry",Cyberscoop, 19 October 2022, https://cyberscoop.com/rob-joyce-nsa-cyber-intel-sharing/.

[155] White House, National Cybersecurity Strategy, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[156] SRMAs are federal departments and agencies to coordinate and collaborate with other departments/agenciesand critical infrastructure operators in each specific sector such as energy, transportation, water and so on.Examples are the Department of Energy (DOE)'s Energy Threat Analysis Center (ETAC), Department of Defence(DoD)'s Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and the NationalSecurity Agency (NSA)'s Cybersecurity Collaboration Center. See https://www.cisa.gov/topics/critical- infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies.

does not mention a detailed specificmodel of information sharing, it requires member States to promote policies underpinning the establishment of cybersecurity-specific Public-Private Partnerships (PPPs) to have an appropriate framework for knowledge exchange, the sharing of best practices and the establishment of a common level of understanding among stakeholders[157].

In regards to mandatory reporting of cybersecurity incidents by critical infrastructure operators, the NIS2 Directive requires member States to mandate essential and important entities[158] to report significant cyber incidents[159] to national computer security incident response teams (CSIRTs) or competent authorities (e.g., national cybersecurity authorities) as well as facilitating the voluntary exchange of information on cyber threats, near misses, vulnerabilities, TTPs, IoCs, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks. In the US, the Cyber Incident Reporting for Critical Infrastructure Act of 2022[160] became effective in March 2022, whichrequires CISA to establish legal obligations to mandate critical infrastructure operators to report significantincidents and ransom payments to CISA within 72 hours. The Act also requires any federal entity receivinga report on a cyber-incident to share that report with CISA within 24 hours, and CISA to share informationto all appropriate entities to the maximum extent practicable, related contextual information, cyber threat indicators and defensive measures.

Another consideration for information sharing is tools to be used to share the information. Both the US CISA Act and the NIS2 Directive recommend the use of automated information sharing systems as manual delivery takes a long time and is not suitable for urgent dissemination of information to a large number of recipients. Moreover, IoCs usually consist of IP addresses or hash values that normally span from 32 to 64 characters, which may involve human errors when being manually entered to cybersecurity solutions (suchas firewalls and intrusion detection systems) from hardcopy papers or document files. Therefore, special means are needed to automatically recognize and reflect threat information by security solutions. There aretwo main streams of representing and transferring threat information in a machine-readable format; Malware Information Sharing Platform (MISP)[161] and Structured Threat Information Expression (STIX)[162].MISP is a threat intelligence and sharing platform to foster the sharing and exchange of information within the cybersecurity community while STIX is a language for expressing cyber threat and observable information

[157] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures fora high common level of cybersecurity across the Union loss, and/or considerable damage to natural or legal persons, entities should report the occurrence of incident with 24 hours, the details of incident (initial assessment on severity/impact and IoCs) with 72 hours and a final report (description, root cause and mitigationmeasures) within a month.

[158] Essential entities and important entities are the operators of critical infrastructure. The distinction between'essential' and 'important' is based on their criticality. See Annex I of NIS2 for a detailed list of sectors.

[159] When a significant cyber incident has been identified which resulted in severe operational disruption, financial loss

[160] US Congress, Cyber Incident Reporting for Critical Infrastructure Act of 2022, PUBLIC LAW 117–103—MAR. 15,2022, 15 March 2022, Pages 990 – 1101, https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf

[161] https://www.misp-standard.org/

[162] https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html

which is to be transferred by Trusted Automated Exchange of Intelligence Information (TAXII)[163], an application layer protocol for exchanging threat information over HTTPS. MISP and STIXhave their own advantages and disadvantages over each other and therefore their popularity/preference varies by sector[164]. For example, the US CISA's Automated Indicator Sharing (AIS)[165] system is based onSTIX/TAXII while NATO's Malware Information Sharing Platform[166] is based on MISP.

As information sharing systems are being used by many users and organizations, they should be operatedin a very secure manner. This is because the systems may contain not only unclassified information but alsosome sensitive/classified information to defend against attackers. When issuing an account for a system, itis important to ensure that only validated individuals/organizations who have passed a sound vetting processare granted access to the system. Additional contents-based access controls may also be required for sensitive information. In case of the cross-border information sharing system used by EU member States, the NIS2 Directive requires ENISA to establish mechanisms to ensure the security and confidentiality of disclosed information and restrict the access, storage, and transmission of such information to intended users. In late 2022, a hacker was granted access to the online portal of InfraGard, a program run by the U.S.Federal Bureau of Investigation (FBI) to build cyber and physical threat information sharing partnerships with the private sector, by masquerading as a legitimate corporate employee and then he/she tried to sell the InfraGuard database at a crime forum[167]. This example shows how important a stringent vetting processis when granting an account.

In addition, when preparing threat information, the sender must determine how the recipient should handle the information. There are two main ways of determining the security level: the first is to use the conventional security labels (such as Top Secret – Secret – Confidential – Unclassified) and the second is to assign the security designations according to the Traffic Light Protocol (TLP version 2.0)[168], with four colours (Red – Amber – Green – Clear) to indicate expected sharing boundaries to be applied by the recipient(s). Security labels are commonly used by intelligence/security/military agencies, and those who have corresponding security clearances are able to have access to the information. This characteristic couldlimit the scope of recipients, making information sharing less useful. Moreover, IoCs, by themselves, maynot be regarded as secret or confidential but the sender may impose some restrictions on re-distribution ofIoCs by recipients. The TLP is an attractive alternative to this conventional security labelling approach, andit is being predominantly

[163] https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html

[164] COSIVE, MISP vs. STIX: What Are The Differences? https://www.cosive.com/misp-vs-stix. (Accessed on 8 May2023)

[165] CISA, Automated Indicator Sharing (AIS), https://www.cisa.gov/topics/cyber-threats-and- advisories/information-sharing/automated-indicator-sharing-ais. (Accessed on 8 May 2023)

[166] NATO, Sharing malware information to defeat cyber-attacks, 29 November 2013, https://www.nato.int/cps/en/natolive/news_105485.htm.

[167] Brian Krebs, FBI's Vetted Info Sharing Network 'InfraGard' Hacked, 13 December 2022, https://krebsonsecurity.com/2022/12/fbis-vetted-info-sharing-network-infragard-hacked/.

[168] CISA, Traffic Light Protocol (TLP) Definitions and Usage, 16 August 2022, https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.

used by a number of CSIRTs and cybersecurity agencies around the globe. Definitions of each colour used in the TLP are shown in Table 3[169].

Color	**Description**
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP: AMBER+STRICT restricts sharing to the organization only.
TLP:GREEN	Limited disclosure, recipients can spread this within their community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure.

Table 3. Definition of Colours in TLP Version 2.0

With the recent increase in ransomware attacks, independent cybersecurity monitoring activities such as Information Sharing and Analysis Centres (ISACs)'s activities for each sector of critical infrastructure, private cybersecurity/IT companies' security services and analyses, and large companies' own private CSIRT activities are gaining more importance. The government should institutionalize these organizationsto share information with the government. Since various agencies within the government dealing with cybersecurity, such as cybersecurity agencies, cyber regulators, national CSIRTs, police agencies, prosecutor's offices, intelligence agencies, and the military, the government should designate a dedicated agency to act as a national Point-of-Contact (PoC) to share information with the private sector and this agency should establish a formal arrangement with the private partners. Otherwise, even if the private sectorreports incidents or shares threat information, there will be inevitable delays or even omissions in collectingand disseminating the information at a national level. For this reason, NIS2 requires member States to designate a single point of contact, and the US Cyber Incident Reporting for Critical Infrastructure Act of 2022 designates CISA as a dedicated institution.

Due to the borderless nature of cyberattacks, it is difficult to respond to global attacks only with national-level information sharing. That is why information sharing at the international level is crucial. International information sharing can occur in various forms. The first form is bilateral or multilateral (such as sharing between national CSIRTs, sharing between cybersecurity authorities, sharing between the military CSIRTs, sharing between intelligence agencies, and sharing between police agencies). This gives the advantage of being able to share information at a detailed level and builds trust between agencies of a same or similar nature. Another form of information sharing is national level bilateral meeting (such as cyber dialogues or forums between Ministries of Foreign Affairs). This type is advantageous since multiple cooperative agendas from various agencies can be discussed at the same time, saving time and coordinating all cyber- related

[169] FIRST, TRAFFIC LIGHT PROTOCOL (TLP): FIRST Standards Definitions and Usage Guidance — Version 2.0, August 2022, https://www.first.org/tlp/.

activities within nations. However, it does present drawbacks, since it may be difficult for Ministriesof Foreign Affairs to monitor and control all cooperative agendas and their outcomes in detail amongst many different agencies. The third approach is to achieve multilateral cooperation via an international information sharing membership (such as FIRST, the global Forum of Incident Response and Security Teams)[170]. This method is beneficial since it provides a means of having a platform to receive informationfrom a large number of organizations around the globe. The advantage of such a large community can be adouble-edged sword, since the information distributed to members may be limited in both quantity and quality because of the difficulty for an organization to have the same level of trust in all members. As eachtype of information sharing has pros and cons, nations should employ all forms to the fullest extent possible.

V. NATO's Current Roles in Cybersecurity

The road that led NATO to the present understanding of applying and expand its capabilities and activities in cyberspace started in 2002, in the Prague Summit, where it was recognized that cyberspace activities could pose a threat to NATO networks.

The needed recognition was strengthened by the cyberattacks to Estonia, becoming the trigger to have a structured approach to posed threats, which was formalized in the Bucharest Summit in 2008, with the issuing of the first Cyber Defence Policy, paving the way for the necessary foundation for the coming developments.

In the Lisbon Summit in 2010, a refined Policy was issued, enabling the forthcoming enhancements regarding NATO posture concerning cyberspace.

At the Wales Summit[171] in 2014, the NATO leaders officially affirmed that cyber defence is part of NATO's core task of collective defence. Two years later, at the Warsaw Summit[172], NATO recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air,on land, and at sea, where all Allies made a Cyber Defence Pledge[173] to enhance their cyber defences. Fromthat moment each ally become responsible for its own cyber defences, such as protecting its CIs, building resilience, in the end bolstering its own cyber defences and concurrently NATO's.

As such NATO becomes a platform for Allies to consult on cyber defence issues, share information on cyber threats, exchange best practices, and coordinate activities, including the following examples[174]:

- Sharing real-time threat information through a dedicated MISP (Malware Information Sharing Platform), as well as exchanging best practices on responding to cyber threats;
- Maintaining rapid-reaction cyber defence teams that can be sent to help Allies;
- Developing targets for Allies to facilitate a common approach to cyber defence capabilities;

[170] https://www.first.org/

[171] NATO, "Wales Summit Declaration," September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[172] NATO, "Warsaw Summit Communiqué," July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[173] NATO, "Cyber Defence Pledge," July 8, 2016, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

[174] NATO, *Fact Sheet: NATO Cyber Defence* (August 2020), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf.

- Investing in education, training and exercises, such as Cyber Coalition[175].

This new Domain also opened new doors, and as foreseen in the Tallinn Manual 2.0[176], Rule 71, a destructive cyberattack to Critical Infrastructures (CIs) of one country by another can be regarded as the same as an armed attack depending on its scale and effect, which accordingly with International Law (IL) could trigger the victim country's right to self-defence.

Being this the case, the natural assumption would be that an attack on an NATO Member could be a reasonable reason for an Ally to invoke the Article 5 of the NATO Treaty, having always in mind that a decision as to when it would lead to the invocation of Article 5 would always be taken by the North Atlantic Council on a case-by-case basis[177]. Under Article 5 of the NATO treaty, when any Ally becomes the victimof an armed attack, it will be considered an attack on all Allies, and they will take collective defence measures. NATO's stance against malicious cyberattacks was further extended at the Brussel Summit[178] in2021, where NATO leaders recognized that the impact of significant malicious cumulative cyber activities might be considered amounting to an armed attack. The term "cumulative" may imply, by some authors, that several low-impact cyberattacks by the same adversary can be regarded as the same as a destructive cyberattack[179].

In this regard the conduction of cyber operations and its infusion in the military planning was somethingthat was deemed as necessary, just as in the Crisis Response Measures (CRM). The required approach should be, in the aforementioned context, framed worked in a common and recognized approach, which made NATO give a step in publishing the AJP-3.20, Allied Joint Doctrine for Cyberspace Operations, in 2020, which become the first guidance, doctrine, for NATO commanders, staffs and forces to plan, executeand assess cyberspace operations (CO) in the context of Allied joint operations.

By 2022, NATO in the Madrid Summit, through its Heads of State and Government, NATO adopted a new strategic concept, reaffirming the key purpose of the Alliance in ensuring the collective defence and its compromise to operate in all domains of operations.

In the overall, and picking up again the NATO Strategic Concept of 2022, we can find the required connection between the Operational Domains under the following defined three core tasks, as defined by NATO based on the 360-degree approach:

- Deterrence and defence.
- Crisis prevention and management; and
- Cooperative security.

[175] Cyber Coalition is the NATO’s annual collective cyber defence exercise which has been held annually since 2008.See: https://www.act.nato.int/cyber-coalition.

[176] Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed. (New York: Cambridge University Press, 2017). The Tallinn Manual, initiated and maintained by the NATO CooperativeCyber Defence Centre of Excellence (CCDCOE), is a comprehensive tool/resource on international law to cyber operations

[177] NATO, Wales Summit Declaration

[178] NATO, *Brussels Summit Communiqué*.

[179] Stefan Soesanto, “When Does a ‘Cyber Attack’ Demand Retaliation? NATO Broadens Its View,” *Defense One*, June 30, 2021, https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/

The Strategic Concept reemphasises "national and collective resilience" as a critical key to all the abovecore tasks, but also stresses the cross-cutting importance of investing in technological innovation, of integrating climate change, human security and overall security, between others, in the Allies agenda acrossall the core tasks.

When focusing on the Maritime and Cyberspace Domain, we can realize, under the defined core tasks,that "Maritime security is key to (…) peace and prosperity" but also that "Maintaining secure use of and unfettered access to (…) cyberspace are key to effective deterrence and defence".

To achieve those goals it is foreseen that a strengthened "posture and situational awareness to deter and defend against all threats" will be required but it will also be needed to "enhance (…) cyber defences, networks and infrastructure". Actions like promoting "innovation and increase investments in emerging and disruptive technologies", are in line with the NATO efforts just like the adoption and integration of new technologies, cooperation with the private sector, and shaping "standards and commit to principles" are. In the overall, all of this actions, will enhance NATO ability to "operate effectively (…) to prevent, detect, counter and respond to the full spectrum of threats, using all available tools" and "uphold freedom of navigation, secure maritime trade routes and protect our main lines of communications". However, NATO is also aware that to deploy capabilities and activities in a maritime engagement space where cyberspace has a crosscut influence, an orchestration needs to be made to have the desired or required effects at the speed of relevance.

From the above realization it could be drawn a commitment from NATO to enhance the overall situational awareness and ensure the security of critical infrastructures, own and of interest, an additional commitment can be seen, namely, to enhance and extend partnerships and cooperation, and all of them having direct repercussion in the maritime and cyberspace domains. Again, it is clear that the aforementioned commitments are in line with the overall demand to attain the required resilience against threats and challenges.

In this long road into the Cyberspace Domain, it becomes also clear that NATO foresees cybersecurityas being an important part of its 360º approach in order to achieve a secure cyberspace and to bolster resilience of the Alliance, of its members and of like-minded nations. This evidence can be visible in someof the below actions, like:

- Defending NATO's own networks and systems from cyberattack, by enhancing its resilience and security, including through the development of standards and practices, also through the useof advanced cybersecurity technologies in conjunction with the private sector to improve the security of critical infrastructure[180];

[180] E.g. with the NATO Computer Incident Response Capability (NCIRC), which protects NATO's own networks by providing centralised and round-the-clock cyber defence support, but also NATO's Cyber Defence ManagementBoard (CDMB) which oversees these efforts. (Reference: NATO, "Cyber Defence," accessed February 14, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm)

- Providing forums[181] for member countries to share information and best practices on cybersecurity, and facilitating information-sharing and cooperation among member countries on cyberspace issues, including through the NATO Cyber Security Collaboration Network, NCIA. NATO also collaborates with other international organizations to promote a coordinatedapproach to cybersecurity[182];
- Supporting allies and partners outside of NATO in their efforts to strengthen their own cybersecurity capabilities, by providing cybersecurity capacity building and technical assistanceto partner countries, e.g. the Defence Education Enhancement Programme (DEEP), but also theNATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) which is a hub for cyberdefence expertise and collaboration, also the NATO Science and Technology Organization (STO);
- Supporting research and development in cybersecurity, including through the NATO Communications and Information Agency (NCIA) and the NATO STO[183]. NATO also collaborates with industry partners to leverage their expertise and innovation in cybersecurity;
- Working with partners outside and within NATO, including international organizations, while promoting with all a coordinated approach through exercises and training events to enhance thereadiness and interoperability of member and like-minded countries' but also to propagate bestpractices and defend against emerging cyber threats.

From all the above it is possible to see how NATO is engaged, and in what could be its compromise to provide a comprehensive understanding of the cyber environment, to enable organizations to makeinformed decisions about their security posture, but also in providing real time threat detection, incident response, and proactive defence all gather in what could be a baseline to an efficient and effective Situational Awareness (SA[184]).

To achieve the required knowledge of the elements in the engagement space it is required to comprehendand understand[185] the current state of the environment but also of the activities within it. This involves collecting, analysing, and interpreting information about the engagement space and its activities to gain a comprehensive understanding of its components, relationships, and potential vulnerabilities. So, and in order to provide

[181] The NATO Cyber Defence Committee (CDC), which is the senior committee responsible for providing guidanceand direction on all NATO cyber defence matters. The CDC is composed of senior civilian and military representatives from all NATO member nations and meets regularly to discuss cybersecurity issues and formulate policy and strategy in the cyber domain. Its responsibilities include overseeing the development of NATO's cyber defence capabilities, identifying and addressing cyber threats, and promoting information sharingand cooperation among member nations

[182] Reference: NATO, "Cyber Defence," accessed February 14, 2023,https://www.nato.int/cps/en/natohq/topics_78170.htm)

[183] Reference: NATO, "Science and Technology," accessed February 14, 2023, https://www.nato.int/cps/en/natohq/topics_50317.htm

[184] A as “The knowledge of the elements in the battlespace necessary to make well-informed decisions”, from theOfficial NATO Terminology Database (https://nso.nato.int/natoterm/Web.mvc)

[185] In the current context, comprehend is seen as perceiving the received information while understand implies adeeper level of insight, like knowledge gained from the received information.

real-time insights of the engagement space, allowing organizations to detect anomalies,identify threats, and respond effectively to incidents will imply, in general:

- Collecting and analysing large amounts of data from various sources, including threat intelligence feeds, to identify patterns, anomalies, and potential threats.
- Analysing and interpreting data, to extract meaningful insights.
- Real-time monitoring and analysis, crucial to detect and respond to threats promptly.
- Continuous data collection, analysis, and dissemination of information to relevant stakeholders.
- Overall risk management processes, by understanding the environment and potential threats, itis possible to prioritize the security efforts, allocate resources effectively, and implement appropriate security controls and countermeasures.

Also, a focus on specific threats and threat actors needs to happen in support of threat detection, incident response, and proactive defence against specific adversaries, this would include potential threats, but also the tactics, techniques, and procedures (TTPs) used by threat actors, and monitoring and studying indicators of compromise (IoCs), to understand the strategies and intentions of adversaries. In general, threat intelligence, will proactively identify emerging threats, understand their potential impact, and develop countermeasures to mitigate or prevent those same threats, contributing understandably for an enhanced SA.

VI. Further Improvement

Considering what has been stated in the previous chapter and implicitly encompassed in the three core tasks as defined by NATO Strategic Concept of 2022, Deterrence and Defence, Crisis prevention and management, and Cooperative security, one could draw the following NATO specific goals, focusing on the Maritime and on the Cyberspace Domains:

- Enhance Information Sharing;
- Develop Cybersecurity Guidelines;
- Invest in Cybersecurity Technologies;
- Foster Public-Private Partnerships;
- Conduct Cybersecurity Exercises.

As an example of where to apply the capacities, activities or develop capabilities, the following examples could be considered:

- Enhance Information Sharing: NATO can facilitate the establishment of Information Sharing and Analysis Centres (ISACs) for port and maritime cybersecurity. These ISACs can promote information sharing and collaboration among stakeholders, including private companies, government agencies, and cybersecurity experts. NATO can also develop common standards and protocols for information sharing and threat intelligence to ensure consistency and interoperability across different ISACs.
- Develop Cybersecurity Guidelines: NATO can develop guidelines and best practices for cybersecurity in the port and maritime sectors. These guidelines can help stakeholders improve their

cybersecurity posture by providing actionable recommendations on threat detection, incident response, and risk management.

- Invest in Cybersecurity Technologies: NATO can invest in research and development of advanced cybersecurity technologies, such as artificial intelligence, machine learning, and blockchain, to enhance the cybersecurity capabilities of port and maritime stakeholders. This can include establishing innovation hubs or partnerships with the private sector to develop andtest new technologies.
- Foster Public-Private Partnerships: NATO can foster public-private partnerships to improve cybersecurity in the port and maritime sectors. These partnerships can enable collaboration andinformation sharing between government agencies and private companies to develop effective cybersecurity solutions that meet the needs of both sectors.
- Conduct Cybersecurity Exercises: NATO can conduct cybersecurity exercises and simulations to test and improve the preparedness of stakeholders in the port and maritime sectors. These exercises can help stakeholders identify gaps in their cybersecurity strategies and develop effective incident response plans.

All these actions could help ensure the safety and security of ports and shipping operations and protect against cyber threats in the evolving threat landscape.

Nonetheless, it is important to stress out the specificities of the public and private “jurisdiction” in these domains, maritime and cyberspace, in order to be able to effectively mitigate cyber threats to the maritime domain. To do this it is important to organize the operating interests of the public and private sector and jurisdictions in a way that maximizes collaboration and information sharing. Some of the ways could be depicted in the following actions:

- Establish Public-Private Partnerships: Governments, port operators, and private companies should work together to establish public-private partnerships that facilitate information sharingand collaboration. These partnerships should be designed to promote a coordinated approach tocyber threat intelligence and response, and should include mechanisms for sharing threat data, best practices, and other relevant information;
- Develop Cybersecurity Guidelines and Standards: The development of cybersecurity guidelines and standards can help to create a common framework for managing cybersecurity risks acrossthe maritime domain. These guidelines should be based on recognized international standards, such as the ISO/IEC 27000 series, and should provide clear and actionable recommendations for managing cybersecurity risks;

- Invest in Advanced Technologies: The public and private sectors should invest in advanced technologies such as artificial intelligence, machine learning, and blockchain to enhance their cybersecurity capabilities. These technologies can be used to detect and prevent cyber threats inreal-time, and can provide valuable insights into emerging threats and vulnerabilities;

- Promote Cybersecurity Training and Awareness: Cybersecurity training and awareness should be a priority for all stakeholders in the maritime domain, including government agencies, port operators, and private companies. This training should focus on developing a culture ofcybersecurity, where all employees understand the risks and are equipped with the skills and knowledge to identify and respond to cyber threats;

- Implement Incident Response Plans: Effective incident response plans should be in place to enable rapid and coordinated responses to cyber threats. These plans should be regularly testedand updated to ensure that they remain effective and relevant.

By organizing the operating interests of the public and private sector and jurisdiction in this way, stakeholders in the maritime domain can work together to mitigate the risks posed by cyber threats, enhance their cybersecurity capabilities, and respond more effectively to emerging threats.

In a lower level of action some of the below detailed examples, could be part of the immediate of proactive measures and effective responses that stakeholders in the maritime domain could take to addressemerging cyber threats:

Proactive measures:

- Conducting regular cybersecurity assessments and audits to identify vulnerabilities and risks in technology assets or systems;
- Implementing effective access control measures such as strong passwords, two-factor authentication, and role-based access control;
- Ensuring that software and hardware are kept up to date with the latest security patches and updates;
- Providing regular cybersecurity training to employees and other stakeholders to raise awareness of cybersecurity risks and best practices;
- Developing and implementing a cybersecurity incident response plan that outlines procedures for detecting, responding to, and recovering from cyberattacks.

Effective responses to emerging threats:

- Implementing a "defence in depth"[186] strategy that includes multiple layers of security controls to detect and prevent cyberattacks;
- Conducting regular penetration testing and vulnerability assessments to identify potential weaknesses in cybersecurity defences;
- Coordinating with law enforcement and other government agencies to investigate and prosecute

[186] Information security strategy integrating people, technology, and operations capabilities to establish variablebarriers across multiple layers and missions of the organization", accordingly with definition from https://csrc.nist.gov/glossary/term/defense_in_depth

cyber criminals;

- Implementing measures to isolate and contain cyberattacks to prevent them from spreading;
- Developing and maintaining backup and recovery strategies to ensure that critical data and systems can be quickly restored in the event of a cyberattack or other incident.

Overall, this proactive measures as such as regular assessments and training could help prevent cyberattacks, while effective responses such as rapid incident detection and containment could help minimize the damage caused by a cyberattack.

VII. Conclusion and Recommendations

Enhancing cybersecurity in the Maritime environment and in the cyberspace domains is of critical importance for NATO and its allies. To address this matter, a proper cyber threat intelligence needs to be in place to allow a timely identification of potential circumstances or events that could adversely impact the Maritime sector. The decision-making cycle must be imbued with the necessary guidance and policiesthat will help facilitate proper acts or to implement necessary measures in order to protect the human-madeassets at Sea, its interfaces with the Maritime environment, and the data associated.

Taking all the above in consideration, the following key conclusions and recommendations can be drawn:

- Collaboration and Information Sharing: Establishing public-private partnerships and Information Sharing and Analysis Centres (ISACs) can promote collaboration and information sharing among stakeholders. Common standards and protocols should be developed to ensure consistency and interoperability.
- Guidelines and Best Practices: Developing cybersecurity guidelines and best practices specific to the Maritime sector is crucial. These guidelines should provide actionable recommendationsfor threat detection, incident response, and risk management;
- Investment in Technologies: Investing in advanced cybersecurity technologies, such as artificial intelligence, machine learning, and blockchain, can enhance the capabilities of stakeholders. Research and development efforts, including partnerships with the private sector, should be pursued to develop and test innovative solutions;
- Training and Awareness: Cybersecurity training (individual and collective, e.g. exercises) and awareness programs are essential for all stakeholders in the maritime domain. Building a culture of cybersecurity and equipping employees with the necessary skills and knowledge will improve overall preparedness;
- Incident Response and Preparedness: Effective incident response plans should be in place, regularly tested, and updated. A "defence in depth" strategy, involving multiple layers of security controls, penetration testing, and vulnerability assessments, will strengthen defences against cyberattacks;

Public-Public and Public-Private Cooperation: Governments, port operators, and private companies should collaborate closely to establish a coordinated approach to cyber threat intelligence and response. Sharing threat data, best practices, and relevant information is essential for a robust cybersecurity framework;

- Standards and Frameworks: The development of cybersecurity standards and frameworks is crucial to managing risks across the maritime domain. These should be based on recognized international standards and provide clear and actionable recommendations;
- Proactive Measures: Regular cybersecurity assessments, strong access control measures, timely

updates of software and hardware, and cybersecurity training are proactive steps that can help prevent cyberattacks;

- Effective Responses: Coordinated responses to emerging threats, including isolating and containing cyberattacks, collaborating with law enforcement, government agencies and the private sector, on implementing backup and recovery strategies, are essential to minimize the damage caused by cyber incidents.

By implementing the above recommendations, stakeholders could strengthen the safety and security of ports and shipping operations, protect against cyber threats, and enhance their cybersecurity capabilities in the evolving threat landscape. A collaborative and proactive approach, along with ongoing investments in technologies and training, will help enable stakeholders to effectively mitigate cyber risks and respond to emerging threats in the maritime domain.

All the above recommendations could become actionable vectors under NATO Strategic Concept of 2022.

DISRUPTIVE IMPACTS ON MARITIME INDUSTRIAL BASE SUPPLY CHAIN AND NAVAL READINESS

Dr. Joshua BEHR

The presentation aims to discuss the disruptive impacts on the supply chains and their implications for naval readiness. The presentation is divided into five parts, covering the premise, the characteristics of supply chains and labor, the concept of the maritime industrial base SoS, the modeling of the SoS, and the resilience of the SoS.

The US has a growing demand for a larger and more durable fleet, which requires a robust infrastructure and a well-functioning maritime industrial base SoS. The SoS is the network of assets and their interrelationships that support naval readiness. However, the SoS is facing various challenges and risks, such as severe weather events, targeted attacks, public health crises, or their combinations. These could have significant consequences for the US and NATO readiness in different regions of the world, such as the Red Sea and the Pacific.

The presenter shows a model of the potential flooding in Hampton Roads, a major maritime industrial base and port area in the US, if Hurricane Sandy had hit the area in 2012. The model illustrates the vulnerability of the critical infrastructure and assets in the area, such as the Norfolk Naval Station, the Allied Command Transformation, and other facilities. The presenter explains the factors and conditions that affect the severity and extent of the flooding, such as the track, the wind speed, and other variables.

The majority of assets and critical infrastructure could be significantly impacted by a hurricane event. For instance, a model event shows the potential damage in the Hampton Roads region, a major maritime industrial base in the US, if a storm similar to Hurricane Sandy were to hit the area. The model illustrates the potential flooding and disruption to the maritime industrial base. Similar risks exist in other areas with robust maritime industrial bases, such as the Gulf Coast region and southern Louisiana.

Currently, the maritime industrial base is near its maximum capacity for repairing and outfitting ships. Any additional, unanticipated repairs could create significant challenges due to the existing backlogs in public and private yards. For instance, extended efforts at sea or responding to multiple crises worldwide could result in more wear and tear on ships and unexpected repairs.

Furthermore, large storms often lead to the displacement of skilled labor from the region, which could exacerbate the current labor shortage. For example, in the aftermath of a storm, it could take weeks, months, or even over a year for the region to recover and return to normal. During this time, some of the displaced labor might not return to the region. This, combined with a potential public health crisis, could put the maritime industrial base in a very difficult position.

The maritime industrial base is a system of systems (SoS) defined by critical assets and their dependencies. It consists of numerous assets, each having relationships with others, forming smaller systems within the larger SoS.

In the Hampton Roads region, there is a need for a model that captures the SoS of the maritime industrial base. Such a model can help identify weak or critical points in the system, guiding investment and prioritization decisions. However, building this model requires identifying the critical infrastructure, which is not straightforward due to differing opinions among various organizations, institutes, government bodies, and industry sectors.

Assuming the critical infrastructure can be identified, the next step is to understand the relationships, dependencies, and interdependencies among these infrastructures. This process requires data collection, which is crucial for building a valid and meaningful model. With a reliable model, it's possible to understand the relationships among the assets and characterize the risk to these assets. For instance, the model can predict the ripple effect across other assets if one asset is compromised. However, the usefulness of the model heavily depends on the validity of the data.

The methodologies developed for Hampton Roads and other maritime industrial base ecosystems in the US and potentially useful for other NATO partners are briefly introduced. The main challenge is to obtain valid data that characterizes the system of systems (SoS) in the maritime domain.

The approach is based on creating dependency functions among the assets in the critical infrastructure, such as fuel, skilled labor, materials, equipment, fiber, chain of command communications, etc. These dependency functions are color-coded according to their intensity and confidence levels.

The data is collected from different segments of the population in the maritime ecosystem, who have different levels of knowledge and visibility of the system. A secure and visual interface is provided to the participants, who can select any two assets in the region and draw an arc to indicate the dependency between them. The participants can also adjust the slider and the radio button to register the strength and the confidence of the dependency.

The methodology developed for Hampton Roads and other maritime industrial base ecosystems involves creating dependency functions among the assets in the critical infrastructure. These functions, which include fuel, skilled labor, materials, equipment, fiber, chain of command communications, etc., are color-coded according to their intensity and confidence levels.

Data is collected from different segments of the population in the maritime ecosystem, who have varying levels of knowledge and visibility of the system. A secure and visual interface is provided to the participants, who can select any two assets in the region and draw an arc to indicate the dependency between them. The participants can also adjust the slider and the radio button to register the strength and the confidence of the dependency.

This methodology allows for the identification of the relative criticality among the assets. Some assets are more critical than others, and their failure could have a multi-directional cascading effect across the region. This information can help prioritize investments to harden these facilities and make them more secure. The ultimate goal is to enhance the resilience of the maritime industrial base and ensure its readiness to face various challenges and risks.