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

MARITIME CRITICAL INFRASTRUCTURE PROTECTION (MCIP)

"MARITIME CRITICAL INFRASTRUCTURE PROTECTION (MCIP) IN A CHANGING SECURITY ENVIRONMENT"

www.marseccoe.org

NATO OTAN

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

Authors: Diren DOĞAN, **Cdr.** (TÜR N) Deniz ÇETİKLİ

First Edition, İstanbul, October 2023

Editor-In-Chief : Capt. (TÜR N) Nazif BOZKURT

Published By
Maritime Security Centre of Excellence (MARSEC COE)

Cover & Graphic Designer
Muhammet Görkem YAYLALAR, Mehmet ADATAŞ

Proof Reading
İsmail ÖZTÜRK

Designer Assistant
Emre ŞİMŞEK

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

51 Pages;

ISBN: 978-975-6786-64-2

Edition: 1

DIRECTOR's REMARKS

In an era of increasing complexity and interdependence, the 21st century stands as a testament to human progress, marked by remarkable technological advancements and societal transformations. Yet, alongside this progress, new vulnerabilities and threats have emerged, threatening the very fabric of societies. Nowhere are these risks more evident than in the realm of critical infrastructure, the backbone of modern societies and the lifelines of economies.

This infrastructure, whether physical or cyber, has become a prime target for various threats, each with its potential to disrupt our way of life. A prominent domain under this umbrella of critical infrastructure, and one that is of paramount importance to global trade and communication, is the maritime domain. Often referred to as the "blue economy," it is a vast network that facilitates global economic activity, underpinning over 80% of international trade. The protection and resilience of this maritime critical infrastructure have become an urgent priority, particularly in an era where hybrid threats are the new norm.

In this comprehensive study, we delve deep into the intricacies of protecting maritime critical infrastructure. The study is rooted in a qualitative research methodology, utilizing a wealth of resources and literature, alongside expert insights drawn from the workshops conducted by the Maritime Security Centre of Excellence (MARSEC-COE) in 2021 and 2022. Our focus is not only on understanding the risks and threats but also on exploring practical solutions to ensure the resilience of this infrastructure.

We begin by unraveling the concept of critical infrastructure, before zooming into the maritime domain to understand its role and vulnerabilities. We examine key challenges, including cyber threats, terrorism, hybrid strategies, and physical threats, and their implications for maritime critical infrastructure. Drawing on the work of the MARSEC-COE, we also scrutinize areas such as Maritime Critical Infrastructure, Critical Energy Infrastructure, Underwater communications cables, and Harbour Protection.

While the threats we face are complex and multifaceted, this study seeks to emphasize the power of cooperation and shared strategies in confronting these challenges. From NATO's strengthened resilience commitment to the launch of the NATO-EU Task Force on Resilient Critical Infrastructure, we highlight examples of collective efforts to enhance maritime critical infrastructure protection.

We invite you, the reader, to journey with us through this important exploration. We hope this study not only illuminates the importance of safeguarding maritime critical infrastructure but also inspires further dialogue and action towards ensuring the resilience of our interconnected world. We stand on the precipice of a "grey century," characterized by complexity. The challenges ahead are formidable, but with clarity of understanding and collective resolve, we can navigate these uncertain waters with confidence and resilience.

Mehmet Cengiz EKREN
Capt. (TÜR N)
DIRECTOR OF MARSEC COE

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

by
Diren DOĞAN[1] – Cdr. (TÜR N) Deniz ÇETİKLİ[2]

1-) PhD Candidate in International Relations is a lecturer in Alanya Alaaddin Keykubat University, International Relations Department. **diren.dogan@alanya.edu.tr**

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

TABLE OF CONTENTS

"Because we are only as strong as our weakest link."

NATO Secretary General Jens Stoltenberg's speech at the event of NATO'S outlook towards 2030 beyond (2021)

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 NATO Maritime Security Centre of Excellence (MARSEC-COE) in 2021 and 2022, publications produced by Centres of Excellence working under the umbrella of NATO, and academic publications.

All these works are essential 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.

Diren DOĞAN
Academic Advisor

RESEARCH METHODOLOGY

Methodology

This study aims to analyze the protection of critical infrastructure and critical energy infrastructure with a focus on maritime environment. The study utilizes a qualitative research methodology, which includes the analysis of existing literature and resources, as well as data gathered from presentations made by MARSEC COE'S workshops, conferences, and Exercise MARSEC findings.

Literature Search

The literature search process involved conducting a comprehensive search for academic articles, research papers, and reports related to critical infrastructure and critical energy infrastructure protection in the maritime environment. The search was conducted using various databases such as Google Scholar, JSTOR, ScienceDirect and NATO or its affiliated centres. The keywords used in the search included "maritime critical infrastructure protection," "critical energy infrastructure," "maritime security, "energy security," "critical infrastructure security," "Maritime Situational Awareness and "CIP/CISR."

MARSEC COE Activities

The MARSEC COE activities provided valuable insights into the current challenges and threats facing critical infrastructure in the maritime environment. The presentations were analyzed to identify the key issues, trends, and emerging threats. The information gathered from the presentations was used to develop an understanding of the current state of critical infrastructure protection in the maritime environment. In this study paper, three separate workshops held in 2021 and 2022 were analyzed. These workshops were held on the tittles of "Maritime Critical Infrastructure Protection", "Protection of Maritime Transportation Infrastructures (Pipelines, LNG Routes, and Subsea Cables)" and "Harbour Protection as a part of CIP&CEIP)". For this reason, in this study paper, Maritime Critical Infrastructure, Critical Energy Infrastructure, Underwater communications cables, and Harbour Protection, which are more intensively addressed by these workshops, are discussed as sub-headings. At the same time, MSA course records were analyzed and included in the study.

Data Analysis

The data collected from the literature search and MARSEC COE presentations were analyzed using content analysis. This method involved coding and categorizing the data to identify key themes and patterns. The themes and patterns identified were used to develop a comprehensive understanding of critical infrastructure protection in the maritime environment, with a focus on critical energy infrastructure.

Key Findings

In conclusion, this study utilized a qualitative research methodology, which included a literature search and analysis of discussions/findings MARSEC COE events, to analyze the protection of critical infrastructure and critical energy infrastructure in the maritime environment. The study identified various challenges and threats facing critical infrastructure in the maritime environment, including cyber threats, terrorism, hybrid strategies, and physical threats. The study also highlighted the importance of cooperation and the need for a comprehensive and mutually shared strategy to protect critical infrastructure in the maritime environment. NATO's strengthened resilience commitment and the launch of the NATO-EU Task Force on Resilient Critical Infrastructure are examples of collective efforts that can enhance critical infrastructure protection in the maritime environment. The study also highlighted the importance of situational awareness and risk analysis in developing a crisis early warning system for critical infrastructure protection and suggested focusing on ensuring the safety and resilience of critical infrastructure, beyond the protection of these fields. In this context, MARSEC COE's "Maritime Security Modelling Project" will enable decision-makers to better understand the MCIP issue in the coming period[1].

(1) Announcement on MARSEC COE Maritime Security Modelling Project www.marseccoe.org/2023/06/09/marsec-coe-maritime-security-modelling-project/

1.Introduction to Critical Infrastructure and Maritime Critical Infrastructure

"We, as Allies, have committed to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. Any deliberate attack against Allies' critical infrastructure would be met with a united and determined response. " [2]

"We can theoretically withdraw from Lebanon; we cannot withdraw even in theory from our reliance on the U.S. electric power grid, the computer and telephone communications systems, or our internal transportation networks..." America's Hidden Vulnerabilities Center for Strategic and International Studies (CSIS), 1984. [3]

This quote reflects a common emphasis among the definitions of critical infrastructure (CI). Although each actor, from individual to country even to international organizations, has a subjective definition of critical infrastructure, the fact that they cannot be dispensed with, let alone that their inadequacy would cause serious problems, is the common content of the definitions of critical infrastructure. Critical infrastructure, which consists of systems that perform important functions of a country or region and affect the life of a community, covers almost every area, from a city's water network to the huge underwater communication cables that pass through the Pacific. Although CI operating in such a comprehensive framework, in all areas of life and interdependently, has a different sector for each country, generally accepted CI sectors are listed in figure 1. Each CI sector is considered highly important in terms of its field of activity and the sectors it affects. However, these include lifeline sectors usually defined as sectors that ensure the continued operation of critical business and government functions and provide vital services that, if compromised or not promptly reinstated, may put human health and safety or national and economic security at risk. These industries offer products and services that are essentially ubiquitous but can create life-threatening conditions in the event of a short-term absence. While the four lifeline sectors may vary for each country or region, it is seen that especially the energy, water, transportation, and communication sectors are common to many actors. [4]

(2)Statement by the North Atlantic Council on the damage to gas pipelines', accessed 3 January 2023, https://www.nato.int/cps/en/natohq/official_texts_207733.htm .
(3)K. Ann Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States, Critical Infrastructure Protection Project, George Mason University (United States of America, 2006), 44, https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf
(4)Constance H. Lau and Beverly Scott, 'Strengthening Regional Resilience: Final Report and Recommendations', National Infrastructure Advisory Council, 21 November 2013, 14. ; Carol V Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', USAWC Press, November 2022, 3.

Figure 1: Critical Infrastructure Sectors [5]

As mentioned before, each actor has a definition of CI within the scope of its own priorities and agendas. However, specifically addressing the CI definitions of several important actors, and NATO's especially, is important.

"Within NATO, Critical Infrastructure is a general term describing a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political, and/or social life on which a nation and/or NATO depends and from an Allied Command Operations (ACO) perspective, critical infrastructure is categorized into three different sub-categories Critical National Infrastructure (CNI), Mission-Vital Infrastructure (MVI) and Key Infrastructure (KI). " [6]

According to this definition, it is seen that NATO considers the concept of CI from the perspective of allied countries on the one hand, on the other hand, it carefully focuses on CI that may create a disadvantage for the operational power of the Alliance. Two key NATO documents published in 2022 also show traces of strategies for critical infrastructure: in the NATO 2022 Strategic Concept:

"We will pursue a more robust, integrated, and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security, as a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty. We will work towards identifying and mitigating strategic vulnerabilities and dependencies, including with respect to our critical infrastructure, supply chains, and health systems." [7]

Similarly, the NATO 2030 document emphasizes that, in line with the CNI sub-category, necessary support would be provided for the protection of CI upon the request of the allied countries in order to increase the resilience of the Alliance.[8] Besides NATO, the EU defines CI as;

"a system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." [9] According to EU Council Directive 2008;

(5)'Critical Infrastructure Facts Page', accessed 3 January 2023, https://www.networkintegritysystems.com/critical-infrastructure.
(6)Ronald S Bearse, 'Introduction to Critical Infrastructure Security And Resilience (CISR)'.
(7)'NATO 2022 Strategic Concept', accessed 3 January 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.
(8)'NATO 2030: United for New Era', 39, accessed 3 January 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.
(9)'Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance)', Text, https://webarchive.nationalarchives.gov.uk/eu-exit/https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114 (Queen's Printer of Acts of Parliament), accessed 3 January 2023, https://www.legislation.gov.uk/eudr/2008/114/article/2.

in order for the damage to the CI of an EU member state to be considered within the scope of "European Critical Infrastructure (ECI)", the deterioration of the relevant CI must affect at least two member states.[10] The International Criminal Police Organization (INTERPOL) uses an effective definition of "Critical infrastructure as the life support system of our everyday existence." and for critical infrastructure, they emphasize that the monitoring/control facilities created by the merger of the digital and physical worlds also pose a significant security vulnerability. [11] For this reason, the awareness of vulnerabilities in sectors of critical infrastructure, particularly in light of the rising new generation threats of the current century, has prompted states to take a proactive approach towards protecting themselves.

Within the context of the MARSEC COE, CI can be defined as the essential assets, facilities, systems, networks, and processes that support the security, safety, and stability of maritime operations. It is possible to deal with this chain of definitions initiated with international actors on the basis of countries, but these definitions will not go beyond the repetition of similar statements since the core definition of CI in every country includes physical/cyber systems and assets that are of vital importance to them and their inadequacy or destruction will have a negative impact on public health, safety, and social life, especially on the physical/economic security of the relevant country. [12]

In other respects, similar CI elements exist with different risk potentials in various areas of the state. One of these areas is the maritime environment. Maritime critical infrastructure (MCI) is part of a country's national critical infrastructure.[13] Maritime critical infrastructure protection (MCIP) refers to measures taken to ensure the security and resilience of maritime infrastructure essential to the functioning of a country or region. These measures include such as safeguarding ports, shipping routes, chokepoints, offshore energy installations, Sealines of Communication (SLOC) etc. along with ensuring the security of the information and communication infrastructures that underpin these operations. MCI constitutes one of the cornerstones of maritime security because it plays a critical role in ensuring the safety and security of maritime operations, and MCIP is held in a special position in the security strategies of countries since threats in the sea area are more difficult to prevent than threats on land.[14] Especially in the post-Cold War period, the multidimensional transformation of security and the emergence of new threat perceptions have necessitated the multidimensional consideration of maritime security. Although analytically, there are three dimensions to maritime security: inter-state, maritime

(10)'Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance)', 2.
(11)'The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices', 11, accessed 4 January 2023, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.
(12)Bearse, 'Introduction to Critical Infrastructure Security And Resilience (CISR)'.
(13)Teodora Gechkova, 'Security of Marine Critical Infrastructure', KNOWLEDGE - International Journal 49, no. 5 (15 December 2021): 945.
(14)Salih Bıçakçı, 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'.

terrorism, and blue crime, the complex nature of maritime security threats blurs the line between these distinctions and requires a different perspective on maritime security.[15] The concept of maritime security has attracted attention in security studies after the 1990s in parallel with the changing nature of international relations, and just like the concept of security itself, it does not have a common definition. But, if there is a common judgment for maritime security, it is that maritime security is not a given.[16] In other words, it is not possible to talk about maritime security in the natural situation and it is essential for states to monitor the maritime area for constructing and ideally achieving Maritime Situational Awareness (MSA) so that they can utilize that awareness in pointing out and addressing potential threats or critical vulnerabilities in order to ensure maritime security.[17] Maritime security is also a framework concept because of the sub-themes it contains. In this direction, maritime security has an inclusive quality that covers the fight against all threats arising from state or non-state actors through maritime areas by including many concepts which are defined as threats to lifeline CI in the maritime environment such as energy security, maritime terrorism, climate change, etc.[18] (Figure 2)

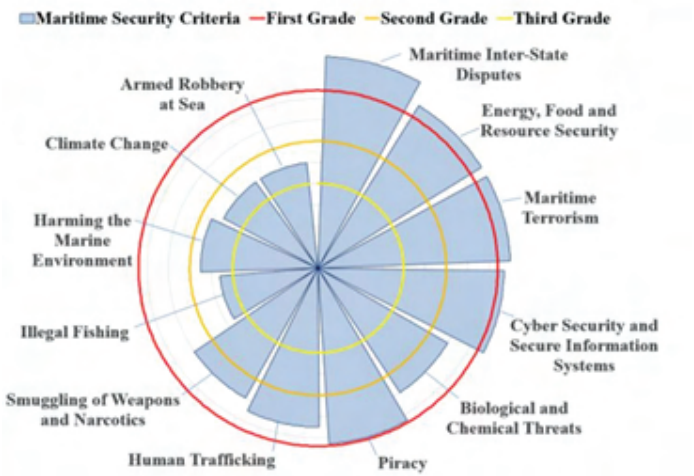


Figure 2: Threats to Lifeline Critical Infrastructure in the Maritime Environment [19]

Along with the awareness of maritime security, the increase in academic studies and the taking of important steps by international actors on maritime security have gained momentum, especially in the current century. The main reason for this situation is that th e incidents of maritime terrorism, which increased in the 2000s, reinforced the collective awareness of maritime areas. At the same time, the oceans, which have served humanity for millennia and provided food and livelihoods to three billion people, have gained more importance, especially with technological developments and globalization.[20]

(15)Müge M. Akar, Aslıhan A. Kemer, and Murat Jane, 'Good Practices in Counter Terrorism in Maritime Domain', Seminar Report (Istanbul, Türkiye: Centre of Excellence Defence Against Terrorism (COE-DAT), 11 October 2022), 3–20.
(16)Arif Bağbaşlıoğlu, 'NATO'nun Deniz Güvenliği Algısı: Süreklilik ve Değişim', Güvenlik Bilimleri Dergisi 10, no. 1 (16 May 2021): 60, https://doi.org/10.28956/gbd.843006.; 'From Fragmented Sea Surveillance to Coordinated Maritime Situational Awareness', 3, accessed 6 January 2023, https://www.marseccoe.org/wp-content/uploads/2022/01/MSA_Study_Paper.pdf.; Mustafa Çakır, 'Güvenliğin Dönüşümü ve Ulusal Güvenlik', The Journal of Diplomacy and Strategy 3, no. 2 (2022): 264, https://dergi-park.org.tr/en/download/article-file/2786023.
(17)'From Fragmented Sea Surveillance to Coordinated Maritime Situational Awareness', 3.
(18)M. Akar, A. Kemer, and Jane, 'Good Practices in Counter Terrorism in Maritime Domain', 23.; Arif Bağbaşlıoğlu, 'NATO'nun Deniz Güvenliği Algısı: Süreklilik ve Değişim', Güvenlik Bilimleri Dergisi, 16 May 2021, 59, https://doi.org/10.28956/gbd.843006.
(19)Oktay Çetin and Mesut Köseoğlu, 'A Study on the Classification of Maritime Security Threat Topics', International Journal of Environment and Geoinformatics 7, no. 3 (6 December 2020): 369, https://doi.org/10.30897/ijegeo.742336.
(20)'While Oceans Cover 70 Per Cent of Earth's Surface, Understanding Has Lagged, Speakers in Lisbon Dialogue Stress, Offering Ways to Close Knowledge Gap | UN Press', accessed 6 January 2023, https://press.un.org/en/2022/sea2152.doc.htm.

And because of the importance placed on the maritime environment, several international actors have placed the notion of maritime security at the forefront of their security strategies. When NATO is analysed as one of these actors; Twenty member countries of NATO, a global actor too, are coastal States that operate twenty ports of global relevance, and eight of the world's twenty largest maritime countries in terms of tonnage are NATO members, four of the world's ten largest shipping companies belong to NATO member countries, and therefore maritime security is an existential priority of the Alliance.[21]

The evidence for this can be seen in the founding Treaty's Articles 5 and 6, which assign the Alliance with the responsibility of collective defense and establish its area of jurisdiction. According to these articles, in the event of an attack on a member, their area of responsibility encompasses the maritime regions of the member states as well as the forces and vessels situated in the North Atlantic area located north of the Tropic of Cancer.[22] In parallel to this, the Strategic Concept published in 2010 and the Alliance's Maritime Strategy announced in 2011 are two important documents showing the focus of the alliance's perspective on the maritime environment. The 2010 Strategic alongside transport Concept's wording and the title "Promoting International Security through Cooperation" emphasize that the alliance recognizes its global role and that NATO's core mission will remain the same as the world changes in the fight against transatlantic global threats.[23] The Alliance's Maritime Strategy which is announced in 2011 states that the alliance aims to maintain flexible naval forces to counter the security threats of the 21st century and defines the following four roles for NATO's naval forces.

1.Deterrence and collective defence;
2.Crisis management;
3.Cooperative security: Outreach through partnerships, dialogue, and cooperation;
4.Maritime security.

In fulfilling these four roles, Allies are expected to maximize the use of new technologies and innovations, including enhanced MSA, encourage greater multinational cooperation and resource pooling, as well as improve organizational structures, operational concepts, doctrine, training, and education.[24] Accordingly, in its Maritime Strategy adopted in 2011, NATO declared that ensuring maritime security is one of the Alliance's main objectives. Similarly, in its 2022 strategic concept, maritime security is emphasized as a key to peace and prosperity and deterring all threats in the maritime environment is set as a core mission.[25]

In the light of all this information, the critical importance of maritime security for NATO includes maritime critical infrastructure, as it refers to the facilities, systems, and networks necessary for the safe and efficient operation of the maritime area. These assets include ports, shipping lanes, oil and gas platforms, communications cables, and other infrastructure vital to the global economy and the security of nations.[26]

(21)Magnus Nordenman, 'The Naval Alliance: Preparing NATO for a Maritime Century' (Atlantic Council, June 2015), 2, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-naval-alliance-preparing-nato-for-a-maritime-century/; Bağbaşlıoğlu, 'NATO'nun Deniz Güvenliği Algısı', 62.; Marcus Lu, 'Ranked: The World's Largest Container Shipping Companies', Visual Capitalist, 26 July 2022, https://www.visualcapitalist.com/worlds-largest-container-shipping-companies-2022/.
(22)Bağbaşlıoğlu, 'NATO'nun Deniz Güvenliği Algısı: Süreklilik ve Değişim', 62–63.
(23)'NATO 2022 Strategic Concept'.
(24)NATO, 'Alliance Maritime Strategy', NATO, accessed 6 January 2023, https://www.nato.int/cps/en/natohq/official_texts_75615.htm.
(25)'NATO 2022 Strategic Concept', 7.
(26)Sümer Kayser, 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'.

Strategies for the protection of these structures are included in the Maritime Security Operation (MSO) concept, which is a sub-heading of the alliance's maritime strategy. (Figure 3)

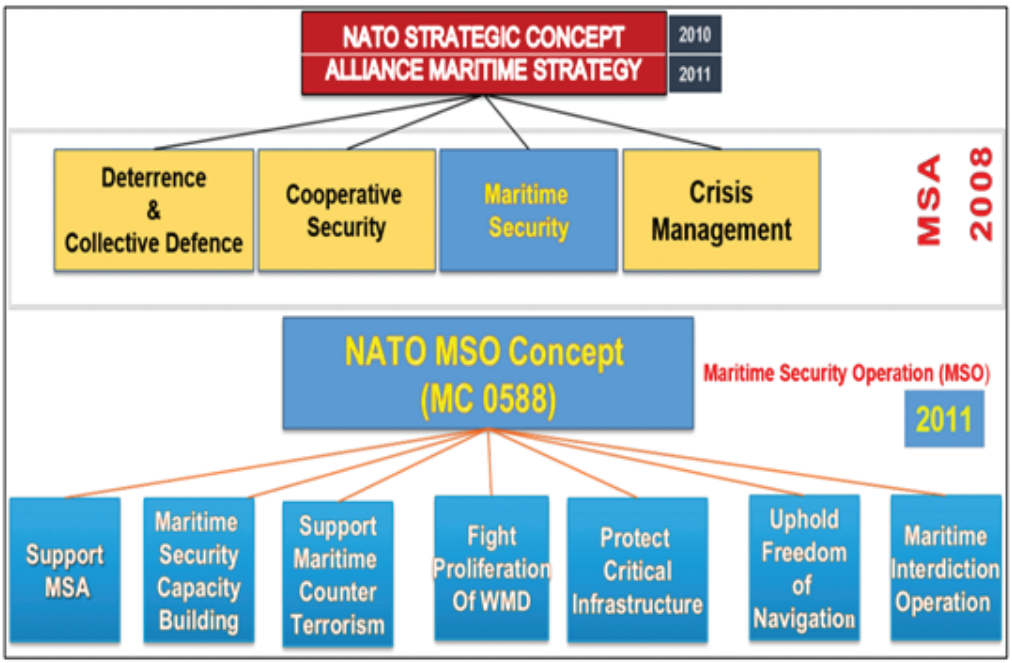


Figure 3: NATO Strategic Concept and Alliance Maritime Strategy[27]

In this direction, at the request of a NATO or non-NATO country and in accordance with directions from the North Atlantic Council (NAC), NATO helps protect CI in the maritime environment, including control of choke points. This mission, together with all its sub-core areas of work and research (Figure 4), aims to develop an awareness of threats and hazards to critical infrastructure, their early detection, rapid response to crises occurring at various choke points, and the development of resistance/resilience for critical infrastructure.

Figure 4: Sub Research Areas in Maritime Critical Infrastructure [28]

1. Security of supply: The strategic chokepoints of maritime energy transportation
2. Protection of maritime transportation infrastructure
3. NATO's maritime operations: Energy security in the maritime environment
4. Vulnerabilities of existing maritime infrastructure
5. Port protection as part of CIP/CEIP
6. Crisis management as Sea/Harbour

(27)NATO Maritime Security Centre of Excellence (MARSEC-COE), 'MARSEC-COE Enlargement Brochure', 2022, 16, https://www.marseccoe.org/published-work/#single/0.
(28)Kayser, 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'.

The strategies for the protection of national and international CI developed for this purpose recognize that it is impossible to protect CI against all kinds of threats completely. In this sense, the protection of CI is essentially a multidimensional risk management practice, and its main objective is to reduce risk to an acceptable level. Likewise, the CI security and resilience strategy is fundamentally based on sound risk management practices.[29] The initial phase of Critical Infrastructure Resilience (CISR) aims to evaluate the level of danger and subsequently implement protective measures meant to decrease that level of danger. When it comes to stakeholders; CISR is first and foremost a national responsibility.[30] Ensuring the security and resilience of these primary functions, which ensure the basic functioning of government and society, is a central responsibility of any state. However, in many countries, as can be seen in the case of ports or power transmission lines, generally all sectors of national infrastructure have been privatized. As a result, the most CI today is owned and operated by private sector businesses, so the primary responsibility for maintaining their infrastructure lies with those businesses. Although operators are primarily responsible for the implementation of safeguards, they usually do so in accordance with instructions or frameworks set by public authorities. Therefore, this is an area where both the state and the private sector need to work together.[31] Due to the importance of the maritime environment and its CI elements, this involves a more sophisticated process. For example, port and maritime security is not only a maritime area security issue, but also part of a broad ecosystem such as cybersecurity, energy security, and CI security.[32] When CI in the maritime area is considered, this ecosystem includes a much larger scale. (Figure 5)

Figure 5: CIP on Maritime Environment

1. Mega-Ports & Mega Terminals
2. Offshore Platforms
3. Undersea Internet Cables
4. Oil Fields
5. Oil Rigs
6. Pipelines
7. Refineries
8. Tankers (Land and Sea)
9. Power Generation Plants
10. Chokepoints
11. Sea Lines of Communication (SLOC)

As the table illustrates, MCIP is essential to ensure the security and resilience of the maritime infrastructure that generally supports the economic activity and daily life of a country or region. At this point, CI in the maritime area is listed mainly in the fields of energy, communication, and transportation. Considering that more than a quarter of the oil and gas supply is produced offshore today, 99% of international data is transported by underwater communications cables, and 90% of international trade is carried out by sea, the importance of MCIP's focus on these areas can be understood more clearly.[33] In this direction, some of these points will be discussed in detail in the following sections under the titles of Critical Energy Protection, Undersea Communication Cables and Port Protection in parallel with the themes covered in the MARSEC COE workshops.

(29)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 7-9; Commission of The European Communities, 'Critical Infrastructure Protection in the fight against terrorism', 7.
(30)NATO, 'Brussels Summit Declaration issued by NATO Heads of State and Government (2018)', NATO, accessed 9 January 2023, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
(31)Deniz Çetikli, 'Critical Infrastructure Protection on Maritime Environment' (Presentation, NATO MARSEC-COE, 5 December 2022).
(32)M. Akar, A. Kemer, and Jane, 'Good Practices in Counter Terrorism in Maritime Domain', 20.
(33)'WEO-2018 Special Report: Offshore Energy Outlook – Analysis', IEA, accessed 9 January 2023, https://www.iea.org/reports/offshore-energy-outlook-2018; 'Map of the week – Submarine telecommunication cables', European Marine Observation and Data Network (EMODnet), 23 August 2019, https://emodnet.ec.europa.eu/en/map-week-%E2%80%93-submarine-telecommunication-cables; Kayser, 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'.

2.Ensuring Energy Security: The Vital Role of Protecting Critical Energy Infrastructure in the Global System

Today, energy is a lifeline CI sector that turns the wheels of the global system and plays a leading role in every aspect of our lives. If we deepen this definition, energy contributes to the delivery of essential goods and services that support many homes, businesses, and governments at large. The possibility of power interruption increases the risk of life-threatening situations. Energy forms part of a physical and electronic network that includes interdependencies with other CI sectors, and the disruption caused by this dependency has a high potential to create new problems by affecting other sectors.[34] (Figure 6) From this point of view, energy is a basic requirement for the continuity of not only a country or region but the entire global system.

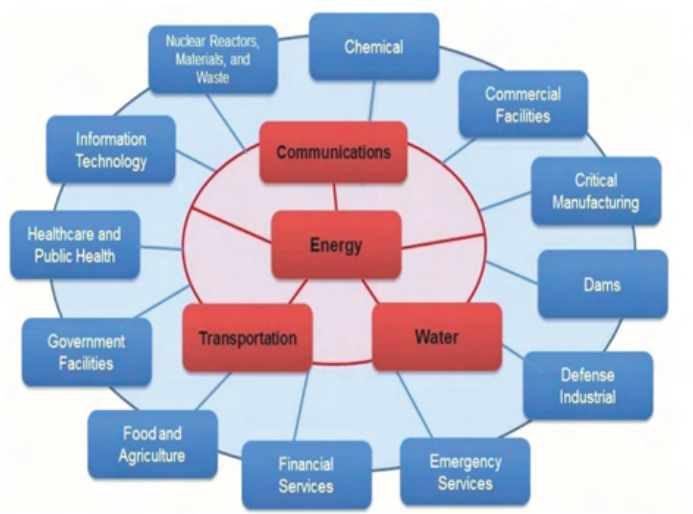


Figure 6: Critical Infrastructure Sectors and Four Lifeline Sectors [35]

Ensuring the energy security, which is in such a vital position, is a prerequisite for its protection. At this point, the definition of the concept of "Energy Security" ranges from the narrow issues of physical supply interruption to broader issues, including the economic, environmental, and political consequences of changes in energy markets. For instance, the International Energy Agency (IEA) defines energy security as the uninterrupted availability of energy sources at an affordable price; achieving this requires efforts to reduce risks to both internal and external energy systems and build resilience to manage residual risks.[36]

At this point, the concept of critical energy infrastructure (CEI) comes to the fore. CEI, which roughly represents all systems used in the generation, distribution, supply and storage of energy; consists of all kinds of facilities that ensure that the materials used as electricity production-distribution-transmission and fuel [coal, liquefied petroleum gas (LPG), liquefied natural gas (LNG), petroleum, nuclear energy raw materials, renewable energy sources (wind, solar, hydroelectric)] are produced in power plants, processed into end-user products and delivered to the consumer, and systems that ensure the management/security of processes in these facilities.[37]

(34)Evans et al,'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)',3
(35)'European Commission SUCCESS Project Report', accessed 11 January 2023, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7096f83&appId=PPGMS.
(36)Dimitrios Dalaklis, 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'; 'Energy Security – Topics', IEA, accessed 11 January 2023, https://www.iea.org/topics/energy-security.
(37)Uğur Özker, 'Türkiye'de Kritik Altyapı ve Siber Güvenlik' (Konrad-Adenauer-Stiftung Türkiye, November 2022), 11, https://www.kas.de/documents/283907/283956/KAS+x-

The elements of critical energy infrastructure are not limited to fixed facilities. Especially in countries like Türkiye, where there is a high percentage of consumers and transit lines, in addition to the pipelines used in transmission, mobile transmission vehicles are also considered among the elements of critical energy infrastructure.[38] The abundance of components comprising Critical Energy Infrastructure (CEI) in this way can heighten susceptibility to various types of threats, rendering it more susceptible to dangers compared to other critical infrastructures. For instance, a power grid may have multiple components, such as transmission lines, substations, and power stations that are all essential to the functioning of the system. A malicious actor may target any of these components, causing the entire grid to fail. Therefore, the complexity and interdependency of CEI components can pose significant challenges for their security and resilience, requiring a comprehensive approach to safeguarding them against potential threats. In this direction, in the report published by the US Department of Homeland Security, the energy sector ranked first among the attacks affecting CI with a rate of 79.32.[39] The main reason why CEI is targeted the most among the threats to CI is that the area of influence and therefore the destructiveness of attacks on energy critical infrastructure is much wider than other critical infrastructure. For instance, a cyber-attack on a power grid can cause widespread power outages that affect homes, hospitals, businesses, transportation, and other essential services. In contrast, an attack on a financial institution may only impact the institution's operations, with limited spillover effects. The scale and interdependency of CEI make it a high-value target for malicious actors seeking to disrupt or destroy critical infrastructure, which can have severe economic, social, and national security consequences. Therefore, protecting CEI against threats requires a robust and multifaceted approach that includes cybersecurity, physical security, emergency preparedness, and recovery planning. Especially today, as systems grow, become smarter, and become more connected by crossing borders, new technologies included in energy grids have invited new generation attack methods.[40] Therefore, CEI also has a special role in other critical infrastructures that provide cross-border or cross-border services and thus affect the interests of many states.[41]

Basically, threats to all CEI sectors are directly related to the national security of states. However, especially with modernization and the use of next-generation systems, electricity stands out a few steps from other sectors. First of all, electricity is one of the three components of total energy production/consumption, alongside transportation and heating.[42] Today, all other CI sectors are heavily dependent on electricity supply (drinking and wastewater systems, food, transport and fuel, healthcare, communications, and financial services).[43] In addition, the awareness of the growing impacts of the climate crisis, a major challenge of our time, has revealed a strong demand for a transition to renewable energy, which has placed an extra role on electricity. Accordingly, world electricity generation increased by 125% from 1990 to 2019, reaching approximately 27 petawatt-hour (PWh) in 2019. In the report presented by the IEA, in order to reduce greenhouse gas emissions to zero by 2050 and limit the increase in global temperatures to 1.5 °C within the scope of combating the climate crisis, renewable resources, which accounted for 29% of global electricity generation in 2020, should reach 90% in 2050. In line with this target, electricity is expected to meet half of the total energy consumption by 2040.[44] As electricity is the key to global energy transmission, it has also become a cornerstone of energy security for all countries.[45] While any supply disruption poses critical challenges, the vulnerability of electricity systems is more urgent.[46]

(38)Bilge Karabacak, 'USAK Kritik Altyapı Güvenliği Projesi Sonuç Raporu', 58, accessed 13 January 2023, https://www.academia.edu/21583796/USAK_Kritik_Altyap%C4%B1_G%C3%BCvenli%C4%9Fi_Projesi_Sonu%C3%A7_Raporu.
(39)Defender Project, 'Defending the European Energy Infrastructures' (Europian Commission, 7 November 2017), 7, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7096f83&appId=PPGMS.
(40)'Grid Resilience: Priorities for the Next Administration', 5, accessed 12 January 2023, https://gridresilience.org/wp-content/uploads/2020/11/NCGR-Report-2020-Full-v2.pdf.
(41)'Critical Infrastructure Resilience: stronger rules', Text, European Commission - European Commission, accessed 12 January 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6238.
(42)Mithat Çelikpala, 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'
(43)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 104.
(44)'Net Zero by 2050 – Analysis', IEA, accessed 14 January 2023, https://www.iea.org/reports/net-zero-by-2050.
(45)NATO, 'Energy security', NATO, accessed 13 January 2023, https://www.nato.int/cps/en/natohq/topics_49208.htm.
(46)'Pathway to critical and formidable goal of net-zero emissions by 2050 is narrow but brings huge benefits, according to IEA special report - News', IEA, accessed 13 January 2023, https://www.iea.org/news/pathway-to-critical-and-formidable-goal-of-net-zero-emissions-by-2050-is-narrow-but-brings-huge-benefits.

At this point, a confronting reality emerges; while electrification is more important in the twenty-first century, including the West world's electricity infrastructure global energy systems remain a product of the twentieth century, posing new strategic challenges to collective thinking about security and resilience.[47] Of course, this sensitivity emphasized for electricity also applies to other critical energy sectors. Herein, a dilemma emerges. In the pursuit of energy system modernization and the establishment of interconnected industrial control systems (ICS), states encounter a paradox. While aiming to align with the demands of the twenty-first century, they inadvertently expose CI to a heightened risk of threats. These threats, capable of impairing the security and functionality of critical energy infrastructure, can be categorized into two overarching domains: natural occurrences and human-made incidents. Examples of such threats encompass information warfare, terrorist attacks, cyber-attacks, technology espionage, accidents, as well as force majeure events including earthquakes, fires, floods, and other natural disasters.[48] (Figure 7)

Figure 7: Threat sources for critical infrastructure[49]

When we evaluated the Colonial pipeline in the USA (2021), Triton in Saudi Arabia (2017)*, and the blackout attacks against Ukraine's electricity systems, see that cyber threats were used more intensively in activities related to critical energy infrastructure recently. This is mainly due to the fact that electricity, oil, gas, and other services are becoming increasingly data-dependent on automated controls to operate their grids.[50] These infrastructure systems are nowadays managed and included in automation with fully automated capabilities through interconnected network systems with the support of Industrial Control Systems (ICS) [Supervisory Control and Data Acquisition (SCADA)/ Distributed Control Systems (DCS) / Programmable Logic Controllers (PLAC)] sensors.

(47)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 103–4.
(48)Hazar Strateji Enstitüsü Hasen, 'Kritik Enerji Altyapı Güvenliği El Kitabı', 13, accessed 14 January 2023, https://www.academia.edu/10027314/Kritik_Enerji_Altyap%C4%B1_G%C3%BCvenli%C4%9Fi_El_Kitab%C4%B1.
(49)Hasen, 'Kritik Enerji Altyapı Güvenliği El Kitabı'.
**Aurora Vulnerability is malicious use of a protective relay or other protection and control device to inflict an out of sync condition that results in physical damage to rotational equipment. Abrupt opening and closing of the protective circuit changes the behaviour of the relay from providing maximum protection to inflicting maximum damage. (Presentation, Energy Security Awareness Course, PfP Training Centre)*
(50)H. Ömer Tunca, 'Defence Industry Infrastructure Protection from Terrorist Attacks: Turkish Experience' (Presentation, Critical Infrastructure Protection from Terrorist Attacks Course, COE-DAT, n.d.).

Many modern power generation plants and organizations rely on data networks to manage meters and analyze their customers' data. The operational processes, control rooms, substations, instrumentation, refineries, and pipelines used to manage facilities now rely on fully digital, video-enabled, high-speed data connections. To manage these processes, data and analytics-centric power generation facilities often use the digital capabilities and analytical tools they have gained in recent years in their core processes such as resource allocation, production optimization, safety control, preventive maintenance, and supply chain planning. For this reason, digitalization is increasingly making the energy sector a more potential target for cyber-attacks.[51]

Aside from the dilemmas posed by energy in our age, in a study which is analyzing energy security, not mentioning maritime energy security and critical energy infrastructure in the maritime environment leads to an incomplete handling of the subject. Maritime infrastructure has grown in several new ways in recent decades. Among the most important changes is the seas' increasing role as a source of energy.[52] In the past, the concept of energy security developed as a result of the need to secure the physical infrastructure and resources of energy. Maritime energy security is an important field that combines energy security and maritime security. Today, however, energy security has taken on the shape of a multidimensional discipline that includes both internal and external actions. Today, when maritime security and energy security are considered, it is important to blend different dimensions and, therefore, to realize and implement political, economic and security measures together.[53]

At this point, the maritime environment includes trade routes, choke points, ships, ports, terminals, pipelines, oil and gas platforms and other critical infrastructure. (Figure 5) Disruption of maritime transport routes and the emergence of threats to maritime security also affect access to maritime energy resources and the security of maritime transport of energy resources. An increasing proportion of energy resources - both oil and liquefied natural gas - are produced offshore and transported by sea.[54] Today, fossil fuels account for more than a third of global maritime trade and half of the world's oil is transported by tankers due to the containerization of international trade. Likewise, LNG is being transported by increasingly larger ships and the increasing share of energy in maritime transport has made maritime transport a cornerstone of globalization.[55] This means that countries are increasingly dependent on the security of energy-critical infrastructure in the maritime environment, which is vulnerable to a range of threats, including terrorist attacks, piracy, and natural disasters.[56]

As in other CI sectors, there are many threat factors affecting energy security and critical energy infrastructure in the maritime environment. Threat factors and threats are two related but distinct concepts when it comes to critical energy infrastructure and energy security. Threat factors are the underlying conditions or circumstances that create the potential for a threat to occur. For example, a country with a history of political instability or terrorist activity might be considered a threat factor to critical energy infrastructure because it creates an environment where an attack on energy infrastructure is more likely to occur. On the other hand, threats are specific events or actions that pose a risk to critical energy infrastructure and energy security. These can include physical attacks, cyberattacks, natural disasters, or other incidents that can disrupt energy supply or cause damage to energy infrastructure.

(51)Özker, 'Türkiye'de Kritik Altyapı ve Siber Güvenlik', 11.
(52)'Maritime Trade: Embracing the Ocean: Delivering the Trade Benefits of the National Shipbuilding Strategy Refresh', n.d.,
(53)Çetikli, 'Critical Infrastructure Protection on Maritime Environment'.
(54)NATO, 'Emerging Threats to Maritime Energy Infrastructure', NATO, accessed 14 January 2023, http://www.nato.int/cps/en/natohq/news_124544.htm.
(55)Caner Öğütçü, 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'.
(56)Çelikpala, 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'.

Terrorist attacks are among these threats. Terrorist attacks pose a serious threat, especially to the waters where energy transport is carried out, areas where offshore energy is extracted, and chokepoints. There is a certain order in the supply-demand process of energy in the world. In order to deliver the energy leaving the supplier as soon as possible, routes with various strategic transit points are used. The points of importance include a passage intensively used for the Asian market, through which 16 million barrels pass daily, another passage connecting the Persian Gulf and the Sea of Oman, through which 21 million barrels pass daily, and a third passage, which plays an important role in the energy transported to Europe, 3.2 million barrels pass daily. (Figure 8)[57] Any terrorist attack on the critical transit routes shown on the map carries a high risk of causing a global crisis. An attack on a maritime chokepoint could disrupt shipping traffic, leading to delays in the delivery of goods and increased transportation costs. This could also lead to a reduction in global trade and a rise in commodity prices.

Figure 8: The World's Key Maritime Chokepoints

For example, an attack on the Strait of Hormuz, which is a critical chokepoint for the transportation of oil from the Middle East to the rest of the world, could cause a spike in oil prices and have significant economic consequences for many countries that rely on oil imports. Likewise, the impact of terrorist attacks on offshore energy platforms will have a much larger multiplier than an attack on land. In this context, special underwater acoustic systems are required to monitor the sea area where the plant is located continuously. This monitoring activity should be carried out both with the underwater acoustic systems of the power plant itself and with the elements of the country's own navy as a whole. Another factor affecting maritime energy security is climate. Climate is an important threat factor that makes its effects on CI felt more and more day by day. One of the world's largest container ships crashed into the shore of the Suez Canal on 24 March 2021 due to poor visibility caused by sandstorms and bad weather conditions. The ship named Ever Given, owned by Evergreen, caused the traffic in the Suez Canal to be closed for six days despite long efforts. During this period, approximately 400 ships waited for the opening of the canal, and the ships that changed their routes traveled through Africa and reached their destination ten days late.[58] While this experience shows the necessity of an update in the content of the critical infrastructure, it has also necessitated a review of the CI in the maritime environment. Because the climate is not the only factor in the Ever Given incident but also the narrow channel and the lack of adjunct measures that can continue the process without interruption in case of obstruction.[59] Where threats to the security of the maritime environment are mentioned, it is not possible to ignore piracy activities as a blue criminal element.[60] On 15 November 2008, the supertanker Sirius Star was carrying 2 million barrels (320,000 m^3) of crude oil when it was hijacked by Somali pirates 450 nautical miles (833 km) southeast of the Kenyan coast. The pirates had set a 10-day deadline and demanded a ransom of USD 25 million.

(57)Çetikli, 'Critical Infrastructure Protection on Maritime Environment'.
(58)'Ever Given: an Example of How Complex International Liability for Damages Can Be', accessed 14 January 2023, https://www.ibanet.org/ever-given-international-liability-damages.
(59)Öğütçü, 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'.
(60)M. Akar, A. Kemer, and Jane, 'Good Practices in Counter Terrorism in Maritime Domain', 3.

The ship and crew were released after a ransom payment of USD 3 million.[61] Similarly, on 18 January 2014, MT Kerala, a 75,000-tonne tanker, disappeared off the coast of Angola. A pirate gang hijacked the vessel, disabled its identification system and communications equipment, and painted over its identifying markings. More than a week later and 1,300 miles away, the pirates released Kerala off the coast of Nigeria after unloading 12,270 tons of diesel cargo to their other vessels.[62] In addition to physical threats to energy critical infrastructure in the maritime environment, emerging cyber threats actually represent a framework concept for threats to all critical infrastructure. Therefore, given the breadth of maritime activities related to the energy sector, cyber security concerns can be grouped in many different ways, just as in other areas. In this study, cyber threats to critical energy infrastructure in the maritime environment are listed as follows:

1. Human Error or Human Ignorance: This type of cyber-attack occurs when crew members make mistakes or lack awareness of cybersecurity risks. For example, they may click on malicious links or download untrusted software on ship systems, leaving vulnerabilities that can be exploited by cybercriminals.
2. Fraud: This type of cyber-attack involves attempts to deceive crew members into disclosing sensitive information or redirecting payments through phishing or scamming. Cybercriminals may pose as legitimate entities and trick crew members into giving them access to sensitive information or diverting payments.
3. Attacks to Facilitate Crime: In this type of cyber-attack, hackers gain unauthorized access to ship systems to steal data, funds, or resources for criminal purposes. These attacks can include maritime theft or piracy and can have significant economic and security implications.
4. Navigational Attacks: Navigational attacks involve manipulating or spoofing computer systems to interfere with navigation. This can include altering Automatic Identification System (AIS) data or Global Positioning System (GPS)of signals, which can have serious safety implications for ships and crew members.
5. Operational Attacks: This type of cyber-attack involves disrupting systems to impair a ship's functioning. For example, cybercriminals may take control of ship systems or disable engines, which can prevent the ship from operating properly.
6. Indiscriminate Attacks: These attacks are large-scale malware or hacking attempts that affect numerous ships or companies in a generalized manner. These attacks are often used to create botnets or mine cryptocurrency using ship resources.[63]
7. Hybrid Attacks: These attacks involve combining multiple attack techniques, such as operational disruption, navigational manipulation, and ransomware. Cybercriminals may use these attacks to cause widespread damage to ship systems or steal sensitive information.
8. Infrastructure Attacks: In this type of cyber-attack, cyber criminals target foundational maritime technologies like AIS, GPS, or communication systems that ships rely on. Disrupting these systems can cause significant problems for ship operations and crew safety.
9. Future Concerns: Emerging attack techniques or technologies that may become more prevalent in the future, such as AI-powered or quantum computing attacks on ship systems. These attacks could have serious implications for the safety and security of the maritime environment.
10. Hybrid Aggression: This type of cyber-attack refers to coordinated cyber and physical attacks against ships or ports by an adversary. These attacks can have significant economic and security implications and may involve multiple actors working together to achieve their goals. [64]

(61)Jo Adetunji, 'Hijacked Saudi Oil Tanker Sirius Star on the Move', The Guardian, 9 January 2009, sec. World news, https://www.theguardian.com/world/2009/jan/09/somalia-pirates-supertanker-ransom.
(62)Çetikli, 'Critical Infrastructure Protection on Maritime Environment'.
(63)A botnet is a network of compromised computers, controlled by a single entity, used for malicious purposes. Infected computers, or "bots," receive commands from a central server to carry out various cyberattacks, such as spamming, DDoS attacks, and data theft.
(64)Ian Ralby and Bochman, 'Cybersecurity concerns for the energy sector in the maritime domain', Atlantic Council (blog), 6 December 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/cybersecurity-concerns-for-the-energy-sector-in-the-maritime-domain/,; Deniz Çetikli, 'Cyber Intelligence in MSO'.

The concept of cybersecurity threats is relatively new for both maritime and energy sectors. The newness and complexity of the critical energy infrastructure in the maritime environment are vulnerable to cyber threats. While the maritime environment is the new playground for cyber attackers, computerized maritime systems are highly vulnerable to cyber threats. This situation reveals cyber threats to the wider sector by focusing on various areas:

1. Harbour / Ports
2. Navigation
3. Rigs
4. Company's Offices / Headquarters (HQ)
5. Threats to maritime vessels [65]

All major systems on ships, submarines, and unmanned vehicles are networked to some extent. Twenty years ago, ships were thought to be isolated, but today this threat is increasing. The privatization of systems and the involvement of non-public actors in energy transport have necessitated joint measures by governments and private sector stakeholders against cyber threats. Cyber-attacks on the maritime sector's operational technology (OT) systems have increased by 900 percent in the last three years, with the number of reported incidents reaching record volumes by the end of the year. Cyber-attacks are becoming increasingly common due to the attractive conveniences they offer, and the relatively low risks involved.[66] Developing resilience against cyber threats is becoming more and more important every day.

The bottom line, protecting offshore infrastructure, energy resources and the security of shipping over the seas affects energy supply security. The security of world coastlines adjacent to major sea lanes of communications necessitates the sustainment of maritime security and they are the ways to have a better energy flow. Awareness is needed to ensure maritime security in energy transportation. Thus, awareness and resilience toward potential risks and threats will be developed. At this point, it is important to be aware of the following four hypothesis:

1. No state or alliance has the capacity and capability to establish and maintain maritime security alone,
2. Once lost, it takes a long and difficult process to restore and maintain,
3. International cooperation and coordination are a must,
4. And the global partnership of regionally provided securities is vital. [67]

Looking at the analyzed concepts from a NATO perspective, it is seen that energy security plays an important role in the collective security of NATO Allies. This situation was formally defined at the Bucharest Summit in 2008 and has since been strengthened:

"We have noted a report 'NATO's Role in Energy Security', prepared in response to the tasking of the Riga Summit. Allies have identified principles that will govern NATO's approach in this field and outlined options and recommendations for further activities. Based on these principles, NATO will engage in the following fields: information and intelligence fusion and sharing; projecting stability; advancing international and regional cooperation; supporting consequence management; and supporting the protection of critical energy infrastructure".[68]

(65)Dalaklis, 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'.
(66)Çetikli, 'Critical Infrastructure Protection on Maritime Environment'.
(67)Çelikpala, 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'.
(68)NATO, 'Déclaration du Sommet de Bucarest publiée par les chefs d'État et de gouvernement des pays membres de l'OTAN (2008)', NATO, accessed 15 January 2023, https://www.nato.int/cps/fr/natohq/official_texts_8443.htm.

For NATO, energy security has gradually become a priority area. Although the alliance has accepted the importance of energy security since the Riga summit, it has come to the forefront of the Alliance agenda, in parallel with the developments in the conjuncture.[69] In this context, NATO's 2010 Strategic Concept underlined that the alliance will contribute to strengthening critical energy infrastructure as a stakeholder in energy security.[70] After the Chicago Summit in 2012, the NATO Energy Security Centre of Excellence (ENSEC COE) was established in Lithuania in 2012. [71] The Wales summits in 2014 was the summits that emphasized the importance of energy security awareness, energy efficiency and protection of critical energy infrastructure for NATO as well as energy security.[72] In the Madrid Summit which convened in the shadow of Russia's invasion of Ukraine in February 2022 and its energy challenge to NATO countries, addressed the themes of energy security, diversification of energy supply and reliable energy supply to NATO's military forces.[73] In the Strategic Concept 2022 adopted at the Madrid Summit, the Allies agreed to invest in capabilities to prepare for, deter and defend against the coercive use of political, economic, energy and other hybrid tactics by state and non-state actors.[74] After all these developments, it is possible to say that energy security constitutes a vital element of resilience for NATO. Accordingly, NATO has divided its role in energy security into three main

1. **Raising energy security awareness** includes intelligence-sharing on energy development, political consultations among Allies, as well as among Allies and partners, and exchanges with outside experts.
2. **Supporting the protection of critical energy infrastructure** is mainly about sharing best practices among experts, organizing training courses, and inserting energy-related scenarios into exercises.
3. **Enhancing energy efficiency in the military** includes the sharing of national best practices, demonstrations of energy-efficient equipment, and the development of military energy efficiency standards. [75]

CEI, is defined by NATO as one of the most vulnerable assets in conflict areas. While it is primarily the responsibility of national governments, as in all critical infrastructure, NATO aims to develop joint strategies to increase the awareness and resilience of its Allies regarding critical energy infrastructure. In this context, the Alliance aims to increase its competence in supporting the protection of critical energy infrastructure mainly through training and exercises. NATO also conducts exercises and shares best practices with partner countries, international organizations, and the private sector, many of which are major energy producers or transit countries. In this regard, the NATO-Istanbul Cooperation Initiative (ICI) Regional Centre in Kuwait has been hosting a course on the protection of critical energy infrastructure since 2018.[76] "Critical Infrastructure Protection in Maritime Domain Course (MOP-MO-25575)" is being held by the NATO-accredited Maritime Security Centre of Excellence (MARSEC COE) in İstanbul/Türkiye, and "Advanced & Basic Level Critical Infrastructure Security and Resilience Against Terrorist Attacks Courses (ACT.397.1 / ACT.936.1)" are executed by the Centre of Excellence Defense Against Terrorism (COE DAT) in Ankara/Türkiye. When we consider maritime security, energy security and NATO's perspective, a relatively new concept emerges: Hybrid threats. Hybrid threats, a concept of the current century, are generally used to describe activities carried out by state or non-state actors below the threshold of war in order to weaken or harm a target through various means.

(69)NATO, 'Riga Summit Declaration Issued by NATO Heads of State and Government (2006)', NATO, accessed 15 January 2023, https://www.nato.int/cps/en/natohq/official_texts_37920.htm.
(70)'NATO Strategic Concept 2010', 17, accessed 15 January 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.
(71)Fresh Media, 'Legal information | NATO Energy Security Centre of Excellence', Legal information | NATO Energy Security Centre of Excellence, accessed 15 January 2023, https://enseccoe.org/en/legal-information/352.
(72)NATO, 'Chicago Summit Declaration issued by NATO Heads of State and Government (2012)', NATO, accessed 15 January 2023, https://www.nato.int/cps/en/natohq/official_texts_87593.htm; NATO, 'Wales Summit Declaration issued by NATO Heads of State and Government (2014)', NATO, accessed 15 January 2023, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
(73)NATO, 'Madrid Summit Declaration Issued by NATO Heads of State and Government (2022)', NATO, accessed 15 January 2023, https://www.nato.int/cps/en/natohq/official_texts_196951.htm.
(74)'NATO 2022 Strategic Concept'
(75)'NATO Review - Energy security: a critical concern for Allies and partners', NATO Review, 26 July 2018, https://www.nato.int/docu/review/articles/2018/07/26/energy-security-a-critical-concern-for-allies-and-partners/index.html.
(76)NATO, 'Energy security'.

The range of tools of hybrid threats is so wide that it includes a wide variety of elements ranging from economic coercion, espionage activities and cyber-attacks to the use of paramilitary elements. In this context, attacks on energy security and critical energy infrastructure also fall within the scope of hybrid threats. Recognizing this, in 2020, the NATO Science and Technology Board officially approved the creation of a research task group that will focus on energy security in the era of hybrid warfare. Thus, it was aimed to identify implicit targets for critical energy infrastructure.[77]

The importance of critical energy infrastructure for NATO is hidden in the opportunities it provides to allies, and the advantages it will provide to competitors in case of damage. At this point, CEI presents potential targets, which could provide an adversary with tempting advantages such as:

1. Disrupting the energy supply just when an unfriendly government does something that is likely to draw NATO's response;
2. Contributing to service disruptions in civilian infrastructure on which the military depends and which may undermine social cohesion;
3. Showing their destructive capabilities to intimidate.[78]

For another reference on critical energy infrastructure in the maritime environment, it is sufficient to refer to NATO's 2011 maritime strategy document. The document emphasizes the role of naval forces in contributing to energy security, including the protection of critical energy infrastructure and maritime lines of communication;" The maintenance of the freedom of navigation, sea-based trade routes, critical infrastructure, energy flows, protection of marine resources and environmental safety are all in Allies' security interests."[79] Furthermore, one of the seven areas identified in the NATO Maritime Security Operations (MSO) Concept is the protection of critical infrastructure, and the planning and execution of NATO MSO-related activities in support of CIP are considered in line with the principles and guidelines for NATO's role in energy security. It is accepted that the protection of CI is a key component in the field of energy security, and information management and sharing in this regard plays an important role in determining the best practices to be applied within NATO. In addition, one of the characteristics of maritime security operations organized by NATO is that they can prevent or deter hostile actions that may affect energy security. In this context, Operation Allied Protector launched in 2009 to enhance maritime security in the waters off the Horn of Africa and Ocean Shield launched in the Gulf of Aden and Indian Ocean against piracy and armed robbery were conducted.[80] Currently Operation Sea Guardian, which has the potential to include all MSO missions, has been carried out in the maritime environment by NATO member countries.[81] While NATO is a security alliance, energy-related developments such as supply disruptions can change the international security environment and have far-reaching security implications for some members. As a result, NATO closely monitors relevant energy trends and developments and seeks to increase strategic awareness in this area. This includes consultations on energy security among allies and partner countries, intelligence sharing, workshops, table-top exercises, and specific activities such as briefings by external experts.

(77)'NATO DERGİSİ - Hibrit savaş döneminde enerji güvenliği', NATO Review, 13 January 2021, https://www.nato.int/docu/review/tr/articles/2021/01/13/hibrit-savas-doeneminde-enerji-guevenligi/index.html.
(78)'NATO Review - Energy Security in the Era of Hybrid Warfare', NATO Review, 13 January 2021, https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html.
(79)NATO, 'Alliance Maritime Strategy'.
(80)NATO, 'Counter-piracy operations (2008-2016)', NATO, accessed 10 May 2023, https://www.nato.int/cps/en/natohq/topics_48815.htm; 'Operation OCEAN SHIELD', mc.nato.int, accessed 15 January 2023, https://mc.nato.int/missions/operation-ocean-shield.aspx.
(81)NATO, 'Operation Sea Guardian', NATO, accessed 15 January 2023, https://www.nato.int/cps/en/natohq/topics_136233.htm.

3.Protecting the World's Information Super-Highways: The Importance of Securing Underwater Communication Cables in the Digital Age

The world today is interconnected like never before, with the internet serving as the backbone of global communication, commerce, and information exchange. However, hidden beneath the vast oceans that span our planet's surface lies a critical yet often overlooked infrastructure that enables this interconnectedness: underwater communication cables. These cables, also known as the "Seabed Highways" or "The World's Information Super-Highways"[82] with 552 active cables today carry more than 98% of international data traffic, cover the globe like a spider web, play a significant role in the transfer of this data and allowing us to send emails, make phone calls, stream videos, and access information from anywhere in the world in milliseconds.[83] (Figure 9) As our reliance on the internet continues to grow exponentially, the security of these underwater communication cables has become paramount**. In the digital age, where cyber threats loom large, safeguarding these cables has become a critical task to protect economies, national security, and daily lives from potential disruption and chaos.

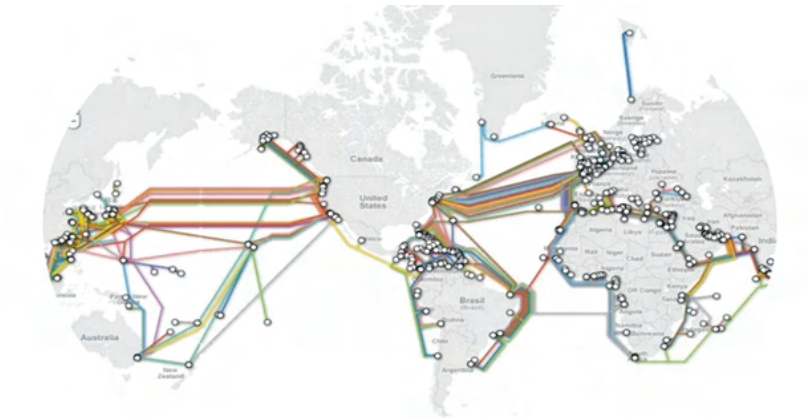


Figure 9: Submarine Cable Map[84]

Underwater communications cables are the technology of choice for rapidly transferring large substantial amounts of data around the world. In addition to underwater cables, satellites are also actively used in data exchange, which accounts for only 1% of data exchange, are costly, and carry data much slower than underwater cables.[85] When comparing underwater communications cables to satellite communication systems, several significant differences become apparent. Underwater cables offer substantial advantages in terms of cost and capacity, with costs estimated to be four times lower and capacity up to twenty times higher than satellite systems.[86] These advantages make underwater cables a popular choice for long-distance communication networks.

(82)Jonathan Hillman, 'Securing the Subsea Network A Primer for Policymakers' (The Center for Strategic and International Studies (CSIS), March 2021), 3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ.
(83)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 93; TeleGeography, 'Submarine Cable FAQs', accessed 16 January 2023, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.
"According to NATO, Critical Undersea Infrastructure defines some systems that underpin vital services, including communications and energy, connecting countries across the globe, mostly via undersea cables. In this direction, NATO Secretary General Jens Stoltenberg announced on 15 February 2023 the creation of a Critical Undersea Infrastructure Coordination Cell at NATO Headquarters.
(84)'Submarine Cable Map', accessed 27 February 2023, https://infoworldmaps.com/submarine-cable-map.
(85)Rona Rita David, 'Submarine Cables: Risks and Security Threats', Energy Industry Review (blog), 25 March 2022, https://energyindustryreview.com/analysis/submarine-cables-risks-and-security-threats/.
(86)Alan Mauldin, 'The Criticality of Submarine Telecommunications Cables' (Maritime Critical Infrastructure Protection Workshop, NATO MARSEC COE, 30 March 2022).

In recent years, satellite internet initiatives such as Starlink, Kuiper, or Telesat have emerged with a primary objective of providing internet access to underdeveloped regions where underwater cables are not feasible or to populations in places where the internet supply has been cut off. These satellite systems can provide internet coverage in remote or underserved areas, including rural or isolated communities, aircraft, and ships, bringing connectivity to areas that previously lacked reliable internet access. This has the potential to bridge the digital divide and empower communities with access to information, education, and economic opportunities. For instance, satellite internet played a crucial role in Iran and Ukraine when their internet supply was disrupted due to political unrest or conflicts. Satellite internet systems provided a lifeline for communication, enabling people to stay connected, access critical information, and communicate with the outside world during these challenging times.

On the other hand, in parallel with the increase in data and usage areas, especially after the Covid-19 period, the laying of underwater cables has been focused on much more intensively than ever before. In addition to a similar rate of data growth demand in the coming years, bandwidth demand is expected to double every two years with the transition to cloud service and the spread of 5G networks.[87] This is because modern communications require substantially more bandwidth than what telegram lines could offer in the nineteenth century. In order to transmit such a massive influx of data, submarine, and terrestrial cables are now composed of fiber optics. Information and data are transmitted as light pulses, which are rapidly emitted through glass fibers across continental telecommunications lines and then between coastal landing stations as the signal travels across the oceans. Such long-haul transmissions also require periodic signal regeneration through amplifiers embedded in the cables' couplers (where lengths of cable are joined together) to ensure that the signal does not dissipate before reaching its destination.[88] In this process, the planning, production, laying, and maintenance of underwater cables are almost entirely in the hands of the private sector. The four largest suppliers as of 2022 are Alcatel Underwater Communications Networks (France), SubCom (USA), NEC (Japan), and newcomer Huawei Marine Networks (China).[89] While network operators have traditionally been the main investors in underwater communications cables, more recently content providers GAFAMs (Google, Amazon, Facebook, Apple, and Microsoft) have also been expanding their investments in this sector to enable the interconnection of data centers.[90] Laying underwater communications cables is a very costly process and processes are usually carried out by establishing consortia. An underwater communications cable can pass through several countries at the same time, so the planning process of cables that will pass through areas with territorial disputes such as the South China Sea can be contentious. Climate change and natural disasters such as earthquakes which will cause damage to the cable planning process, are other factors to be considered. As a result, it is aimed to establish a flexible system that can transfer under all conditions and adapt to the increase in demand.[91]

In this point, considering the confidentiality and importance of the data it carries, underwater cables are as important as other CI such as oil, gas, or electricity. Almost all government traffic, including sensitive diplomatic and military orders, use such cables to reach officials in the field.[92] This situation reveals the necessity of managing and protecting the global underwater communications cable network. On the other hand, aside from the risks and vulnerabilities of these cables, their potential to foster new forms of tension and conflict is too important to ignore.

(87)'Invisible and Vital: Undersea Cables and Transatlantic Security', accessed 16 January 2023, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.
(88)'Factsheet: Submarine Cables – Maritime Awareness Project', accessed 16 January 2023, https://map.nbr.org/2018/07/submarine-cables/.
(89)Jonathan Kim, 'Submarine Cables: the Invisible Fiber Link Enabling the Internet', Dgtl Infra (blog), 5 May 2022, https://dgtlinfra.com/submarine-cables-fiber-link-internet/.
(90)'Invisible and Vital'.
(91)Hillman, 'Securing the Subsea Network A Primer for Policymakers'.
(92)'Cyberspace In Deep Water: Protecting Undersea Communication Cables', 4, accessed 16 January 2023, https://www.belfercenter.org/sites/default/files/files/publication/PAE_final_draft_-_043010.pdf.

To date, networks have been considered mainly in narrow, technical terms, despite their importance for national and international security, geopolitics, state-building, and the development of societies.[93] For this reason, it is possible to say that similar sensitivities have not been shown to underwater communications cables as other critical infrastructures when considering the threats that arise at the point of protection of cables. At least 100-150 underwater cables with a working life of about 25 years are damaged due to accidents or intentional attacks every year. In other words, cable failure occurs on average every three days in any part of the world. Although the number of these accidents, which are mostly caused by fishing and maritime activities, is small, the effects of malicious activities such as piracy are significant.

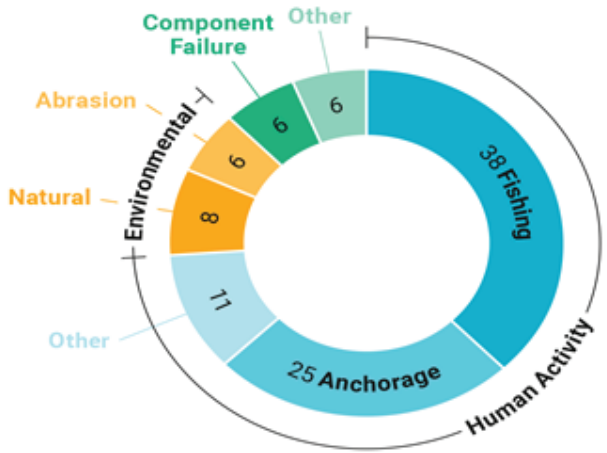


Figure 10: Causes of Underwater Communications Cables Faults[94]

As can be seen from the figure, damages to underwater communications cables are divided into three categories environmental and human-activity induced and other related to technological faults (component failure and other defects).[95] (Figure 10) Climate and natural events, which are in the environmental category, are one of the relatively low probability threats to underwater communications cables, but the damage caused by earthquakes has had a devastating effect. For example, the 6.7 magnitude earthquake on 26 December 2006 triggered a submarine landslide near the junction of the Eurasian and Philippine tectonic plates. The epicenter of the event called the Hengchun earthquake, was located in the middle of the heavily cable-lined Luzon Strait off Taiwan. Submarine landslides following the earthquake severed 9 of the 11 cables in the area, moving them away from their original routes. The work started with eleven cable ships to repair the systems took 49 days to complete. During this period, especially the Asian markets, where the economic flow was fast, remained without the Internet for a long time. This event has been an experience for cable planners to consider seismic points before planning.[96] One of the most common concerns about the destruction of underwater communications cables is the biting of cables by sharks. Although there have been a few biting incidents on cables on the seabed, sharks do not pose a threat to underwater cables. [97]

(93)Ferhat M. Ertosun, '"Protection of Maritime Transportation Infrastructure" (Pipelines, LNG Routes and Subsea Cables)' (Maritime Critical Infrastructure Protection (MCIP) Workshop, NATO MARSEC COE, 30 March 2022).
(94)Alan Mauldin, 'Cable Breakage: When and How Cables Go Down', accessed 16 January 2023, https://blog.telegeography.com/what-happens-when-submarine-cables-break.
(95)TeleGeography, 'Submarine Cable FAQs'.
(96)'Cyberspace In Deep Water: Protecting Undersea Communication Cables', 117.
(97)'TeleGeography, 'Submarine Cable FAQs'.

More than half of the damage to underwater communications cables is caused by ship anchors and fishing nets.[98] In the face of this high rate, cable planners prefer to bury cables on the seabed in fishing grounds to minimize risks. At the same time, there are also actors who take measures within the framework of their laws for the protection of underwater communications cables. For example, Australia and New Zealand have introduced legislation to prevent fishing and damage to cables in the areas through which the cables pass and have strengthened them with sanctions.[99] Disconnections in the event of a cable break are usually compensated for by the supply from other cables; because in most places there are at least two cable systems connected in a ring. However, the situation is not very encouraging for countries that depend on a single underwater communications cable. For example, this happened in Pakistan on 27 June 2005, when the only underwater communications cable connecting the country to the rest of the world was cut due to the entanglement of the anchor of a fishing boat. In the absence of a replacement cable or any recovery strategy, nearly 10 million online subscribers in Pakistan were without internet for more than a week.[100] As can be understood from this example, underwater communications cables are like cotton threads that provide our communication with the world, and if they break, the lack of another thread to replace them has the potential to cause irreversible damage. In addition to these unintentional human-induced activities, there are deliberate cable-cutting activities, albeit at a lower rate, but their effects are high. These are divided into two categories: sabotage and espionage.[101]

In 2007, an important example of sabotage was when Vietnamese fishermen cut an underwater communications cable to buy and resell composite materials. Vietnam thus lost almost 90 percent of its connectivity with the rest of the world for three weeks.[102] Unintentional threats to underwater communications cables are repairable and their destructive effects are tolerable. The main risk to them is the malicious and deliberate activities carried out by state or non-state actors aiming to harm the direct security of states. Though intentional obstruction of connectivity is illegal under international law, today, these activities targeting underwater cables are happening in struggles below the threshold of war under the umbrella of grey zone strategies and hybrid threats.[103] In general, hybrid threats conducted against democratic states by their non-democratic rivals, are a set of corrosive activities that infiltrate the boundaries of international law and are highly deniable.[104] Cyberspace and the maritime environment are potential places for such strategies. This is because the breadth of these domains and the large number of different public and private actors involved make attribution of attacks or damage difficult and blur the line between activities.[105]

The threat potential posed by the secrecy and operational risk of the data carried by underwater cables has also been taken seriously by NATO as an actor focusing on hybrid threats. From NATO's point of view, underwater communications cables are a significant risk, with the possibility of becoming a military target at any time. Aware of this situation, NATO discussed the issues of underwater communications cables and critical maritime infrastructure at the Defence Ministers meeting held on 22 October 2020, and Secretary General Jens Stoltenberg made a press statement after the meeting and stated that threats to underwater cables were taken seriously and closely monitored. [106] In the declaration of the Brussels Summit held in 2021 NATO made this statement;

(98)'ICPC International Call to Action for COVID-19', 6 April 2020, https://subtelforum.com/icpc-international-call-to-action-for-covid-19/.
(99)Hillman, 'Securing the Subsea Network A Primer for Policymakers', 8.
(100) 'Cyberspace In Deep Water: Protecting Undersea Communication Cables', 113.
(101)'Strategic Importance of, and Dependence on, Undersea Cables', accessed 17 January 2023, https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf.
(102)David, 'Submarine Cables'.
(103)Lane Burdette, 'Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy', Journal of Public and International Affairs, accessed 18 January 2023, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy.
(104)NATO, 'Brussels Summit Communiqué Issued by NATO Heads of State and Government (2021)', NATO, accessed 17 January 2023, https://www.nato.int/cps/en/natohq/news_185000.htm.
(105)NATO, 'Allied Joint Force Command Norfolk declares Full Operational Capability', NATO, accessed 17 January 2023, https://www.nato.int/cps/en/natohq/news_185870.htm; Christian Bueger, 'Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU', n.d.
(106)NATO, 'NATO Stands up Undersea Infrastructure Coordination Cell', NATO, accessed 16 May 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.

"We continue to reinforce our maritime posture and to protect our sea lines of communication. We welcome the establishment of the NATO Maritime Security Centre of Excellence in Türkiye. We will maintain awareness of any potential threats to our critical submarine infrastructure and will continue to address them nationally and, where needed, collectively."[107]

In rapid response to the security sensitivity of underwater cables and emerging threats, NATO reactivated the new North Atlantic Command - Joint Force Command Norfolk, based in Norfolk, USA, which opened in September 2020. The Command, established to protect sea lanes between Europe and North America, has been the first NATO headquarters dedicated to the Atlantic since 2003. According to NATO sources, 'one of the tasks of this new North Atlantic Command is also to look into how to protect, how to monitor threats against it."[108] NATO's last statement about the creation of a Critical Undersea Infrastructure (CUI) Coordination Cell on 15 February 2023 is one of the most recent developments on the protection of CUI which includes undersea communication cables.[109] The most important practitioners of hybrid threat activities against underwater cables, which are carefully monitored by NATO, are China and Russia. When these two actors are compared with each other, it is seen that they focus on different areas and perform a kind of job share. Russia pursues a strategy of gathering intelligence from existing underwater cables and cutting them in the event of an escalation to disconnect allies. In addition to the underwater cables visible on open-source maps, it also aims to find underwater cables used for military purposes by conducting scanning activities. China, on the other hand, is pursuing strategies to take part in the production of underwater cables on a larger scale and laying them on the seabed. In this direction, firstly, Russia can access the data on fiber optic cables without damaging it with its specially equipped submarines and thus can listen, scramble, and possibly change the data passing through the cables.[110] Russia's main assistants in achieving such strategic goals are nuclear-powered submarines and oceanographic ships that can carry different equipment or smaller submarine robots.[111] (Figure 11) The names Losharik and Yantar stand out here. The nuclear-powered U-boat "Losharik" is suitable for rescuing downed aircraft, installing listening sensors, and manipulating or bombing underwater communications cables. Losharik suffered a serious accident on 1 July 2019 and is out of service but is expected to be back in service in the next few years. Yantar is a platform that is officially an oceanographic research vessel but is actually the mother ship of surveillance equipment and manned/unmanned deep-sea divers.[112] Yantar entered service in 2015, and since then, the interest in underwater cables by the United States and other NATO countries has aroused suspicion.[113] In the same year, the sighting of Yantar off the US coast near underwater cables caused tension between the two states.[114] Yantar, which carries out operations in many strategic regions from off the coast of Syria to the Persian Gulf, was also reported to have been seen around underwater cables off the coast of Ireland in 2021.[115] Russia's submarine activities focus on gathering intelligence from underwater communications cables as well as monitoring the systems on the seabed.

(107)'Cutting the Cord'.
(108)NATO, 'Allied Joint Force Command Norfolk declares Full Operational Capability', NATO, accessed 17 January 2023, https://www.nato.int/cps/en/natohq/news_185870.htm; Christian Bueger, 'Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU', n.d.
(109)NATO, 'NATO Stands up Undersea Infrastructure Coordination Cell', NATO, accessed 16 May 2023, https://www.nato.int/cps/en/natohq/news_211919.htm.
(110)'Cutting the Cord'.
(111) Andrew Salerno-Garthwaite, 'Seabed warfare is a "real and present threat"', Naval Technology (blog), 20 December 2022, https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/.
(112)'What makes Russia's new spy ship Yantar special?', BBC News, 3 January 2018, sec. Europe, https://www.bbc.com/news/world-europe-42543712.
(113)'Evaluating the Russian Threat to Undersea Cables', Lawfare, 5 March 2018, https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables.
(114)David E. Sanger and Eric Schmitt, 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', The New York Times, 25 October 2015, sec. World, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.
(115)H. I. Sutton, 'Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables', Naval News (blog), 19 August 2021, https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/.

During Russia's invasion of Ukraine, gas leaks occurred in Russia's Nord Stream 1 and Nord Stream 2 pipelines in the Baltic Sea. While the gas leaks in the Swedish field raised the possibility of sabotage on the one hand, they also brought to mind the uncertainty in the detection of attacks on CI and the impact they would have.[116]

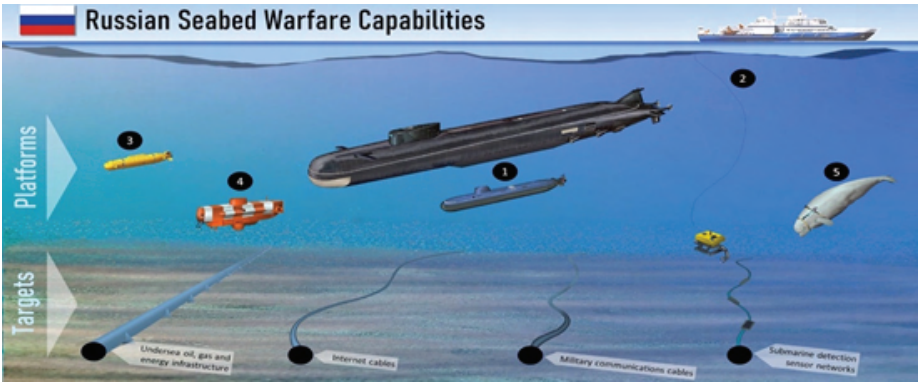


Figure 11: Russian Seabed Warfare Capabilities[117]

Secondly, when it comes to the People's Republic of China, it is essential to remember that we are dealing with one of the best implementers of grey zone strategies and hybrid threats. China's strategy regarding underwater cables appears to be much more long-term. Especially considering its patience and persistence in implementing a salami-slicing strategy, this can be said to be an inference with a high probability of accuracy for China. At this point, China aims to be included in the underwater cable laying system and to direct the system according to its own needs instead of gathering intelligence by reaching the already laid cables or disconnecting the connection like Russia. Therefore, in recent years, Chinese telecommunication companies have started to invest heavily in owning and supplying submarine cables.[118] At least 31 cables newly deployed in 2021 had ownership stakes in these companies. Remarkably, many Chinese investments in the global underwater communications cable network are directly controlled by the Chinese government, as the "big three" Chinese telecommunications companies that invest in underwater communications cables and control 98.5 percent of China's international bandwidth are fully state-owned. These are China Mobile (China Mobile, Zhongguo yidong), China Telecom (China Telecom, Zhongxinguo) and China Unicom (China Unicom, Zhongguo liantong). (Figure 12)

Chinese State-Owned Firm	Investment in Cable to be Deployed in 2022	Cable Touches...
China Mobile	Bay to Bay Express (BtoBE) Cable System	Singapore, Malaysia, China, US
China Telecom	Asia Direct Cable	Philippines, China (2 landing points), Japan, Vietnam, Thailand, Singapore
China Unicom	Asia Direct Cable	Philippines, China (2 landing points), Japan, Vietnam, Thailand, Singapore

Figure 12 : Chinese State-Owned Firms[119]

(116)'İsveç'ten Kuzey Akım 1 ve Kuzey Akım 2 Gaz Sızıntılarında Ağır Sabotaj Tespiti', accessed 17 January 2023, https://www.aa.com.tr/tr/dunya/isvecten-kuzey-akim-1-ve-kuzey-akim-2-gaz-sizintilarinda-agir-sabotaj-tespiti/2742068.
(117)Sutton, 'Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables'.
(118)'Securing Asia's Subsea Network: U.S. Interests and Strategic Options', accessed 17 January 2023, https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options.
(119)'Beijing's Growing Influence on the Global Undersea Cable Network', Jamestown, accessed 18 January 2023, https://jamestown.org/program/beijings-growing-influence-on-the-global-undersea-cable-network/;; Justin Sherman, 'Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security', Atlantic Council, accessed 14 April 2023, 11-12. https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf

In addition to these companies, China has encouraged the private sector champion Chinese companies to take possession of key markets, especially in the field of telecommunications, as part of its "go out" strategy.[120] In line with this strategy, in 2019, Hengtong Group, a private Chinese company that has developed ties with the government, acquired Huawei Marine, the world's fourth-largest underwater communications cable manufacturer, and renamed it HMN Technologies.[121] At the same time, after the Belt and Road Initiative was announced in 2013, it announced the Digital Silk Road (DSR) initiative in 2015 and used these companies as the Trojan horse of its project.[122] China's strategy for underwater cables is basically expressed in these three

1. Global Sabotage (exploiting influence within DSR)
2. Global Espionage (Intelligence gathering using DSR cables)
3. Territorial Sabotage (Manipulating the connection in various territorial disputes such as the South China Sea dispute.)[123]

When China passed through a century of humiliation, left behind the century of recovery, and entered the twenty-first century, it appeared on the stage of the international community with a new image. This image opened a brand-new window to societies that had been exploited, humiliated, or pushed out of the international system due to their low democratic values in previous centuries. China has promised these countries a new world order with attractive themes such as "non-interference in internal affairs", "living together with peace", "win-win", and "common future". Societies that have suffered from these themes in the past have been the first to follow the sound of China's piper. In 2013, when Belt and Road Initiative (BRI) was announced, the societies that opened their doors to Chinese investments were mainly African, Central Asian, and Middle Eastern countries.[124] Similarly, China's DSR initiative has found more demand, especially in developing countries. As a result, China has laid enough cables to encircle the globe, including intercontinental links from Asia to Africa and from Africa to South America.[125] By laying underwater cables to underdeveloped countries, China has developed diplomatic relations with these countries on the one hand and created a digital dependency network against itself on the other. With the DSR, China has sought to erode the dominance of the US, Japan, and Europe in the underwater cable market by turning it into a quest for underwater dominance, while propagating a loosely defined policy directive directed by both bottom-up and top-down forces which blur the lines between public strategy and private action.[126]

These systems, which are being integrated not only in developing regions but also in the European market at artificially low prices, are not only a bridge between the transmitter and receiver of data but also a means of global espionage in peacetime and sabotage in wartime. The statements of a Chinese official clearly summarize this situation; *"Although submarine cable laying is a business, it is also a battlefield where information can be obtained."* The main concern with China's underwater cable laying activity is the ease with which data can be retrieved from these cables. Data can also be siphoned from underwater communications cables. This is most readily accomplished during the cable manufacturing process, when backdoors may be installed to capture data. Similar vulnerabilities exist at onshore landing stations, where cables connect to terrestrial networks, and there is a high probability of cyber security vulnerabilities during the transfer of data.

(120)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 92.
(121)WJI staff and wire services, 'Rebranded Huawei Marine Networks to supply the cable for Asia Link Cable System', accessed 18 January 2023, https://www.wirenet.org/news-categories/item/855-rebranded-huawei-marine-networks-to-supply-the-cable-for-asia-link-cable-system.
(122)'The Digital Silk Road: Introduction', IISS, accessed 18 January 2023, https://www.iiss.org/blogs/analysis/2022/12/digital-silk-road-introduction.
(123)Burdette, 'Leveraging Submarine Cables for Political Gain'.
(124)Christoph NEDOPIL WANG, 'Kuşak ve Yol Girişimi Ülkeleri (BRI) – Yeşil Finans ve Kalkınma Merkezi', accessed 18 January 2023, https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/.
(125)'Mapping China's Digital Silk Road', Reconnecting Asia, 19 October 2021, https://reconasia.csis.org/mapping-chinas-digital-silk-road/.
(126)Burdette, 'Leveraging Submarine Cables for Political Gain'; Yuen Yuen Ang, 'Demystifying Belt and Road', Foreign Affairs, 29 December 2022, https://www.foreignaffairs.com/articles/china/2019-05-22/demystifying-belt-and-road; 'Next battleground in US-China tech war: undersea internet cables', South China Morning Post, 14 December 2019, https://www.scmp.com/week-asia/politics/article/3042058/us-china-tech-wars-new-battleground-undersea-internet-cables.

Finally, data can be retrieved from also cables at sea, though this is relatively difficult to do. Underwater cable laying operations involving private sector partners are therefore more controlled as they involve many actors involved in the process at the same time.[127] Because the companies that finance and own underwater communications cables are not the same as the companies that actually produce them, but the financial backing of the cable owners gives them the power to decide where in which part of the world a cable is laid. It determines where it is connected and how fast (speed, bandwidth) the connection will be made. (Figure 13) As a result, cable owners contribute to the reshaping of the physical layout of the global internet, i.e., the continuous development of servers, cables and other man-made infrastructure that support the operation of the internet.[128] (Figure 14)

State influence via...	The company:	The risks:	Some Chinese firms in question:
Cable owner	Owns and maintain, and may have financed, the cable	Spying on data, disrupting data, shaping cable layout	China Mobile, China Telecom, China Unicom
Cable builder	Builds part of the cable (such as the fiber or the cable itself)	Backdooring equipment	Huawei Marine

Figure 13: Risk Overview of Chinese State Influence through Cable Owner vs Cable Builder[129]

Alongside DSR, China's flagship project is PEACE cable, which aims to provide a cost-effective and diverse route for growing capacity demand between Asia, Africa, and Europe.[130] The PEACE cable, planned to be the shortest route between Asia and Africa, includes landing points in Pakistan, where China recently launched its first direct terrestrial cable, and Djibouti, China's first overseas military base. The entire planned route covers 15,000 kilometers and includes landing points in Kenya and Seychelles, followed by a European connection point in Marseille, France.[131]

From a different perspective, China's 2017 National Intelligence Law and the 2014 Counter-Espionage Law further call into question the independence of companies such as Huawei. Article 7 of the first law states that *"any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law,"* adding that the state *"protects"* any individual and organization that aids it. And the 2014 Counter-Espionage law says that *"when the state security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals shall provide it truthfully and may not refuse."* This law creates the perception of living like a potential intelligence agent among the Chinese people and companies. When China's prevalence in espionage activities is added to this, it is inevitable for states to establish control over companies and reshape the internet through them. [132]

(127) Nadia Schadlow, 'Protecting Undersea Cables Must Be Made a National Security Priority', 3, accessed 18 January 2023, https://www.hudson.org/national-security-defense/protecting-undersea-cables-must-be-made-a-national-security-priority.
(128)'China builds undersea cable bases amid digital infrastructure rivalry', South China Morning Post, 12 December 2021, https://www.scmp.com/news/china/diplomacy/article/3159328/china-builds-undersea-cable-bases-amid-digital-infrastructure.
(129)Andrea Ratiu, 'Cyber defense across the ocean floor: The geopolitics of submarine cable security', Atlantic Council (blog), 13 September2021,https://www.atlanticcouncil.org/in-depth-research-reports/port/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/.
(130)'PCCW Global signs up to extend PEACE cable to southern Africa', Capacity Media, 20 January 2020, https://www.capacitymedia.com/article/29otbyvgrerkbxkdezmrk/news/pccw-global-signs-up-to-extend-peace-cable-to-southern-africa.
(131)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 95.
(132)Arjun Kharpal, 'Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice', CNBC, accessed 18 January 2023, https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

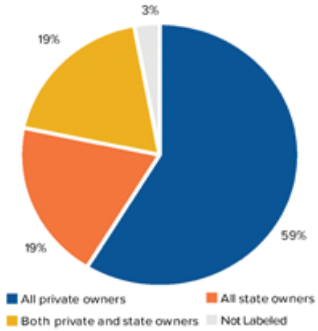


Figure 14: Cables Public-Private Ownership Breakdown (2020)[133]

China can also use underwater cables on issues defined as its red lines. The South China Sea dispute, the most complex territorial dispute in the international system with at least five claimant states, is one of the most suitable areas for such Chinese behavior. Against China's sovereignty claims in the South China Sea (SCS), which it aggressively defends with its historical U-shaped map and Four Sha doctrine, easily sabotaged underwater cables would be a deterrent threat. For other countries in the SCS, which China does not hesitate to punish through economic coercion and sanctions, being ready for China's activities at any time is an important reflex. Similarly, a scenario of sabotage to 14 underwater cables before China's possible invasion attempt against Taiwan, which China recognizes as its own territory, would cause Taiwan to be cut off from communication with the world and unable to call for help from its allies.[134] The Asia-Pacific region, which attracts more attention day by day, especially in the axis of great power rivalry, is also a strategic place where hybrid threats turn into a field of activity with its micro conflict areas. Of course, it is important to remember that underwater cables are the weak point of not only the countries experiencing regional conflicts but also all sovereign and autonomous countries. It is imperative for states to build resilience in this area to ensure their intelligence security and strengthen their strategic communication capabilities. Diversification of underwater cables, increasing intelligence sharing among allies, filling the missing areas in the context of international law, producing emergency scenarios, developing resilience against the capital power of foreign companies, strengthening the ability to monitor and track cables, and developing cyber capabilities are elements that can contribute to the development of resilience.

(133)"Data is Revolution", https://www.thestrategicfunds.com.pr/data-is-the-revolution/ (31 October 2022)
(134)Philip Heijmans, Cindy Wang, and Samson Ellis, 'Taiwan tensions raise alarms over risks to world's subsea cables', The Japan Times, 31 October 2022, https://www.japantimes.co.jp/news/2022/10/31/asia-pacific/taiwan-tensions-subsea-cables/.

4.The Strategic Importance of Harbour Protection in the Maritime Industry

Approximately 70 percent of our planet comprises oceans, which have been servicing humanity for thousands of years. By technological improvements and globalization, the effect of the maritime environment on lives is getting more important. Many important cities in the world owe their origins and prosperity to ports. Ports and maritime trade are important drivers of urbanization. By 2035, it is expected that more than half of the world's population will live in coastal areas and depend heavily on the exchange of goods through ports.[135] At the beginning of 2020, the total world fleet reached 98140 commercial ships and a capacity of 2.06 bl. dwt. The fleet grew by 4.1 percent in 2020, the highest growth rate since 2014, according to the United Nations Conference on Trade and Development (UNCTAD) Reports.[136] Such expansion and developments in the maritime field increase the strategic importance of ports and harbours. Due to their importance, depending on their size, structure, and volume transshipped harbours can be part of the CI of countries and require special treatment and attention when it comes to their protection and security. Destruction of harbour infrastructure can not only adversely affect the political, economic, or social life of a given community, but can also undermine the strategies pursued by a state. Security and defence are, therefore, one of the most fundamental needs for the normal and effective functioning of the harbour industry.[137] In this respect, before examining strategies for the protection of harbours, it is important to emphasize the difference between harbour and port. A harbour is a place on the coast where ships, boats, and barges can take shelter in stormy weather. A port, on the other hand, is a man-made infrastructure on the coast that can be used to transport, load and unload cargo. A port is located inside a harbour, but a harbour cannot be located inside a port.[138] Therefore, the concept of "harbour protection" also includes the security of the port inside the harbour. The protection of national critical infrastructure, especially harbour infrastructure, is a matter of strategic importance for ensuring the full scope of the country's national security.

Figure 16: Types of Harbour

In a MSA scenario, two main areas of interest can be recognized, harbour protection and navigation safety. Harbour protection is currently the main concern and is intended to control the risk related to possible attacks or illegal activities that may take place in maritime access areas.

On the other hand, the objectives of navigation safety are essentially linked to achieve improved maritime navigation awareness by providing information on collision avoidance and general guidance to mariners.[139]

(135) 'The Role and Relevance of the Maritime Domain in an Urban-Centric Operational Environment', 8, accessed 18 January 2023, https://www.coecsw.org/fileadmin/content_uploads/projects/Role_and_Relevance_of_the_Maritime_Domain _in_an_Urban-Centric_Operational_Environment.pdf.
(136)'Review of Maritime Transport 2020', UNCTAD, 2020.
(137)Teodora Gechkova and Tiana Kaleeva, Harbour Infrastructure Protection – PESTLE ANALYSIS', KNOWLEDGE - International Journal 49, no. 5 (15 December 2021): 961–64.
(138) Ertosun, '"Protection of Maritime Transportation Infrastructure"(Pipelines, LNG Routes and Subsea Cables)'.
(139)Amerigo Capria et al., 'Multifunction Imaging Passive Radar for Harbour Protection and Navigation Safety', IEEE Aerospace and Electronic Systems Magazine 32, no. 2 (February 2017): 30, https://doi.org/10.1109/MAES.2017.160025.

The harbour, as a component of the critical infrastructure, is subjected to different negative aspects that affect its everyday activities and provision of services. Harbour security encompasses security and law enforcement measures to safeguard a seaport from terrorism and other unlawful activities, measures employed to ensure international codes and treaties are enforced, and security of commercial areas in and around ports, coastlines, and beaches.[140] A successful attack on a harbour can cause serious economic and military damage, provide an enemy with the opportunity to inflict mass casualties, and have serious long-term detrimental effects on the national economy.[141] The best-known example of this is the terrorist attack by Al-Qaeda on the destroyer USS Cole, anchored in the Port of Aden on the Arabian Sea coast of Yemen, on 12 October 2000. In the attack, 17 sailors lost their lives, and 42 sailors were injured. This action, which was carried out by two suicide bombers using fast fiberglass boats, has gone down in history as the first terrorist attack on a warship in the world.[142] Another example related to harbour security is the Mumbai Attacks of 26-29 November 2008. The Mumbai Attacks carried out by the Lashkar-e-Taiba terrorist organisation were multidimensional attacks because they included the Taj Hotel, CS Terminus, Trident Hotel, Colabai Ville Parle, Jewish Cultural Centre, Cruz Airport, and several hospitals. In the 60-hour-long gunfight, 10 Lashkar-e Taiba militants clashed with security forces, and nine out of ten were killed. Militants had killed about two hundred people in three days of attacks.[143] Despite these significant and high-profile attacks, terrorists rarely choose the sea route due to limited resources and capabilities. Apart from the problem of resources and capabilities, terrorists prefer buses, subways, and trains over maritime means of transport because they attract media attention and are easy targets. In addition, maritime transport is not usually the first choice or main source of transport for most people. And maritime transport is not regarded as "iconic targets" in line with the general tenets of terrorism, like propaganda and resound. Therefore, although maritime routes are generally not the first choice of terrorists, Harbour security is also affected by this reality as digital transformation expands the scope of security.[144] As the examples illustrate, MCIP faces many challenges in an asymmetric environment.

Harbour and maritime security are not only related to maritime security issues, but also to energy security, CI security and the efficiency of global trade. Therefore, cyber security, energy security, harbour security and CI security are together parts of the maritime security eco-system.[145] Harbours, as one of these components, are highly vulnerable to many threats due to their size, general accessibility by sea and land, heavy material and human traffic, being located in densely populated areas, etc. At the same time, since they represent a large number of transport routes (roads, railways, navigation channels), they are much easier targets for terrorist attacks than other regions.[146] The fact that terrorists have historically gained experience in land-based attacks means that a terrorist group aiming to inflict damage in the maritime environment may target areas that lack maneuverability and mobility, such as harbour facilities.

(140)Susan SIM, 'Port Security'.
(141)Robert B. Watts, 'Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment', Homeland Security Affairs 1, no. 2 (2005): 1, https://apps.dtic.mil/sti/pdfs/ADA484165.pdf.
(142) M. Kağan Kozanhan and İbrahim Bayezit, 'Terrorist Threat with Improvised Explosive Device (IED) in the Marine Environment and Its Effects on Maritime Security', Güvenlik Stratejileri 16, no. 34 (2020): 341, https://doi.org/10.17752/guvenlikstrtj.768616.
(143)'Lessons From the Mumbai Terrorist Attacks', accessed 21 January 2023, https://www.govinfo.gov/content/pkg/CHRG-111shrg49484/html/CHRG-111shrg49484.htm.
(144)SIM, 'Port Security'.
(145) M. Akar, A. Kemer, and Jane, 'Good Practices in Counter Terrorism in Maritime Domain', 20.
(146)Ferhat M. Ertosun, 'Harbor Protection as Part of CIP/CEIP (Critical Infrastructure&Critical Energy Infrastructure Protection)'.

Planning to protect harbours from terrorists should take into account attacks from a range of platforms available to malicious actors, including divers, fast boats, jet skis, shipping containers and remotely piloted boats.[147] Although the main threat to harbour facilities is terrorism, other categories of threats include:

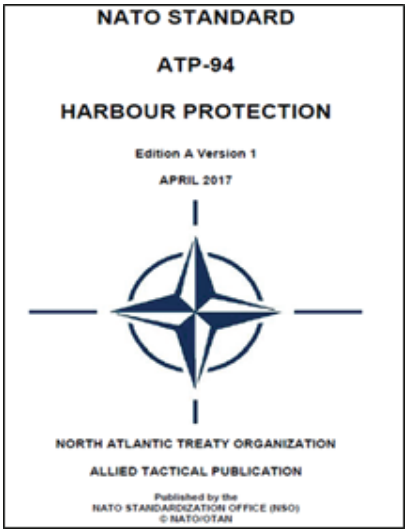
Figure 17: General Threats for Harbour Infrastructure

- Thefts from ships and harbour installations;
- Terrorism, bomb attacks, hostage situations;
- Traffic of forbidden substances;
- Sabotages, intentional damage or destruction of harbour installations, of the communications network, of the data communication network, of a part of a ship, equipment or cargo, vandalism;
- Piracy and armed robbery;
- Threats against the environment: accidental spillage or intentional drainage of pollutants;
- Proliferation and development of terrorist networks, transnational organized crime, illegal traffic persons, etc.

As listed above, there is a wide range of threats to harbours. Especially with the acceleration of globalization, the emergence of non-state actors and their targeting of harbours while carrying out terrorist activities for ideological purposes has activated global actors. Foremost among these is NATO, an Atlantic Alliance whose Members count also 26 coastal States. Many CI facilities in NATO member states are located along the coastline, including oil and gas terminals.[148] These harbours provide a target rich environment for malicious actors; using the right target, in the right place, at the right time, with the right threat vector, can cause great damage to port facilities and the communities and economies they support.

This has driven NATO to focus its port protection strategy not only on protecting the harbours of member states but also on protecting harbours in countries where the "host nation" is unable or unwilling to protect NATO forces. For this reason, NATO established the Specialist Team on Harbour Protection (STHP) in 2012. STHP started its activities under the leadership of Portugal and in partnership with the Centre of Excellence for Operations in Confined and Shallow Waters (COE CSW) accredited by NATO in 2009. The main objective of the Expertise Group is defined as "enhance the ability of maritime forces to adequately cope with asymmetric threats in missions abroad, especially when they are most vulnerable - while entering and leaving or staying in a port." The work of the Expertise Team resulted in the Allied Harbour Protection Publication, which was submitted for approval in 2016. The approval process was finalized with the Allied Tactical Publication (ATP)-94 published in 2017. [149]

(147)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 33.
(148)Evans et al., 32.
(149)'COE-CSW - CENTRE OF EXCELLENCE for Operations in Confined and Shallow Waters: Another Milestone in Harbour Protection', accessed 18 January 2023, https://www.coecsw.org/our-work/spotlights/archive/another-milestone-in-harbour-protection/.



The purpose of ATP-94, NATO Harbour Protection, is to provide the philosophy, principles, and background information on Harbour Protection Operations (HPO) and to give NATO Expeditionary Forces a common basis for its conduct to provide protection for units, facilities and infrastructure while keeping ports' normal routine operations. The document is generally based on the approach that NATO capacity to project and sustain operations directly affects its success. Promptness and effectiveness of NATO operational responses rely heavily on strategic mobility, which, in turn, is highly dependent on the unimpeded movement of supplies, equipment and personnel along the sea lines of communication (SLOC). However, the protection of the SLOC is not sufficient to ensure the safe and timely delivery of logistic support to military operations as ports of departure and arrival are usually the most vulnerable points. As more than 90 percent of all military cargo enters an Area of Operations (AOO) via Sea Port of Disembarkations (SPOD), these spots are key for strategic mobility, requiring a non-threatening or substantially benign environment. Ensuring essential port operating routines brings forward the need to carefully address safety and security measures to cover for the landward and seaward protection of ships, harbour approaches, and anchorages especially against asymmetric threats. However, Harbour protection is not merely about the protection of ships in port. Although it is primarily aimed at the support of forward-deployed NATO forces, it can also be employed to assist a third party in keeping critical maritime services and infrastructures working normally. NATO would thus be able to create favorable conditions to ensure the normal flow of goods into a troubled area, foster the confidence of maritime operators and provide relief to local communities.

The doctrine introduces HP core elements and illustrates the HP organizational backbone architecture, tasks and responsibilities of key players and legal considerations to be addressed in host nation agreements. [150]

(150)Audrius Venckunas, 'Harbour Protection Doctrine'.

Harbour Protection (HP)	• HP encompasses the safety and security measures to cover the landward and seaward protection of units, facilities and critical infrastructures located in port/harbour areas and associated anchorages used in support of expeditionary operations, while keeping routine port operations running.
Harbour Protection Operation (HPO)	• HPO is the combined activity of Harbour Defence and Port Security.
Harbour Protection Commander (HPC)	• An operational experienced staff officer assigned by the Officer in Tactical Command (OTC) to exercise command/control of forces conducting harbour defence/port security tasks. • The HPC is responsible for employing assigned forces in a layered defence and for coordinating efforts of supporting force

Figure 18: Definitions from ATP-94

Integral parts of the doctrine are based on the availability of a Harbour Protection Module (Figure 19) is an integrated, deployable, modular, interoperable, and armoured system of systems and can be employed ashore or embarked on a ship (berthed or at anchor). The HPM combines sensors and C2 systems as well as effectors to detect, identify and counter threats in all domains while at the same time providing interface function to communicate with own tactical units at sea, on land and in the air as well as with civilian stakeholders. While the system itself is still in procurement, a demonstrator HPM was provided by the Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research (WTD 71) was tested in the summer of 2015 during a major Portuguese naval maneuver in Portimão, the largest port on the Algarve coast.[151] As well as in several Northern Coast Exercises in the Baltic Sea from 2013 to 2018. In a complex scenario, the system was technically audited by WTD 71 but operated by the Portuguese as well as The German Navy as a demonstration of its suitability for international use. These and other findings, including identified shortcomings, were recorded and utilized in the further development of the HPM and the associated technical regulation. Likewise, these findings have also formed the basis for the development of ATP 94 and have been updated by the STHP in the context of various workshops and conferences.[152]

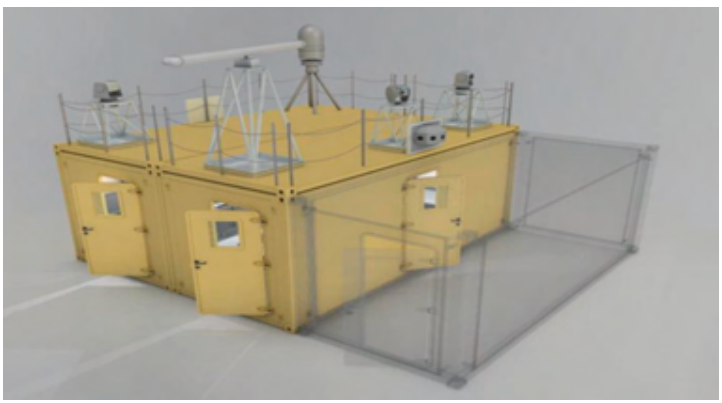


Figure 19: Harbour Protection Module (HPM)

(151)Venckunas.
(152)'European Security & Defence', 44–47, accessed 18 January 2023, https://euro-sd.com/wp-content/uploads/2021/04/ES-D_02_2019_WEB-1.pdf.

The defence of a naval ship anchored in a harbour is a complex task influenced by many factors a topic which is picked up in another NATO doctrine, ATP 74 (Allied Maritime Force Protection), which focuses, among others, on threats against naval units at sea, in confined waters, harbour and respective countermeasures. These mainly include the density of fishing vessels close to the ship and the difficulty of separating neutral ships from threats. A naval ship anchored in harbour is more vulnerable to attack than a ship on the high seas. The chances of detecting and countering a terrorist threat vary greatly depending on several factors, including early identification of the attack and other measures that are currently ready.[153] In this context, the protection of national critical infrastructure, in particular harbour infrastructure, is a matter of strategic importance for the comprehensive provision of national security. In order to achieve this, states need to carry out an inclusive harbour protection strategy by utilizing all areas of technology. However, this also means opening the door to new threats. For example, the digital transformation of ports leads to an increase in cyber-attacks. The Antwerp attack in June 2011 based on malware infiltration into the port system, the Rotterdam attack in June 2017 was related to the collateral damage caused by a large-scale infection, the Long Beach attack in 2018, Barcelona attack in 2018 was related to contamination of internal IT systems, highly sophisticated cyberattack to San Diego in 2018, the cyberattack amidst geopolitical conflict in Shadid Rajaee on May 2020 were among these cyber-attacks influence harbour security.[154] The challenge of building and maintaining secure, resilient harbours is undoubtedly compelling. However, significant investments of thought and resources, the development of advanced situational awareness capabilities for a common operating picture, and the deployment of effective threat countermeasures and state-of-the-art protection systems are helping to ensure the security of major ports. This achievement represents some of the best CISR efforts in several countries.[155] Within the framework of the stated threats, risks, and measures related to port security; it is becoming increasingly difficult to ensure the necessity of achieving higher efficiency standards and sustainability. Because in the future, attacks on the maritime transport system will be multimodal (i.e., hybrid) attacks that include both cyber and physical components. In this context, it is clearly understood that technological developments have changed all the dynamics of port security to ensure the balance between trade facilitation and security. The responsibility of nations is to follow all developments sensitively, revise their security policies and strengthen the resilience of their critical infrastructure. Port protection is also at the forefront of these.

Another important point is to emphasize the importance of the International Ship and Port Facility Security (ISPS) Code[156] when discussing harbour and port security. The ISPS Code is a global maritime security framework established by the International Maritime Organization (IMO) in the aftermath of the 9/11 terrorist attacks. It aims to provide a standardized, consistent approach to maritime security, ensuring the safety of ships and port facilities worldwide. The ISPS Code comprises two parts: Part A outlines mandatory security-related requirements for governments, port authorities, and shipping companies, while Part B provides guidance on implementing those requirements. The Code applies to all ships engaged in international voyages, including passenger ships, cargo ships of 500 gross tonnage or more, and mobile offshore drilling units, as well as to port facilities serving such ships.

(153)Ertosun, 'Harbor Protection as Part of CIP/CEIP (Critical Infrastructure&Critical Energy Infrastructure Protection)'.
(154)SIM, 'Port Security'.
(155)Evans et al., 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)', 34.
(156) The International Ship and Port Facility Security (ISPS) Code is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on Maritime security including minimum security arrangements for ships, ports and government agencies.

Key aspects of the ISPS Code include:

1) Risk assessment: The ISPS Code requires a comprehensive security assessment to identify potential threats, vulnerabilities, and risks at both the ship and port facility levels. This assessment informs the development of a Ship Security Plan (SSP) for vessels and a Port Facility Security Plan (PFSP) for port facilities.

2) Security levels: The Code defines three security levels, with Level 1 representing normal security measures, Level 2 indicating heightened security measures due to an increased risk of a security incident, and Level 3 requiring the implementation of additional security measures in response to a specific security threat or actual security incident.

3) Security officers: The ISPS Code mandates the appointment of a Ship Security Officer (SSO) for each vessel and a Port Facility Security Officer (PFSO) for each port facility. These officers are responsible for implementing, maintaining, and updating their respective security plans.

4) Training and drills: The Code requires regular security training and drills for crew members and port facility personnel to ensure their readiness to respond to security incidents.

5) Access control: The ISPS Code emphasizes the importance of controlling access to port facilities and ships, implementing measures such as identification checks, restricted areas, and security personnel to prevent unauthorized entry.

6) Monitoring and surveillance: Effective monitoring and surveillance systems, including the use of CCTV cameras, security patrols, and alarms, are crucial components of the ISPS Code to detect and deter security threats.

The ISPS Code plays a vital role in harbour and port security by providing a comprehensive and standardized framework for assessing risks, implementing security measures, and ensuring the preparedness of both ships and port facilities to respond to security incidents.

5.Conclusion

In conclusion, the protection of critical infrastructure (CI) in the maritime environment is a complex and multifaceted challenge that requires a comprehensive and collaborative approach. While the pursuit of perfect protection may be unattainable, governments and organizations should prioritize increasing the resilience of CI against evolving threats. This can be achieved through the adoption of flexible and adaptable strategies that focus on mitigating risks, ensuring continuity of operations, and facilitating swift recovery from disruptive events.

The concepts of Critical Infrastructure Security and Resilience (CISR) and Critical Infrastructure Protection (CIP) play crucial roles in safeguarding CI. Both CISR and CIP are important elements of overall CI security, and both are critical for ensuring the continued functioning of CI systems in the face of disruptions. CISR refers to the ability of CI to withstand and recover from disruptive events, such as natural disasters, cyber-attacks, or physical attacks. This includes measures to ensure the physical protection of CI assets and enhance the resilience of CI systems to ensure they can continue to operate in the face of disruptions. CIP, on the other hand, refers specifically to the protection of CI against physical and cyber threats. This includes measures to secure CI facilities, systems, and networks, as well as the development of incident response plans to deal with security incidents affecting critical infrastructure. In general, there are three main requirements for a successful Critical Infrastructure Protection (CIP) policy for states: the identification of risks to themselves, the identification of vulnerabilities, and the enhancement of their resilience to uncertain future threats, such as pandemic disasters, climate-related events, malicious activities, and more.

In the modern interconnected world, where almost all CI sectors provide essential services to societies, the absence or disruption of these services can have far-reaching and unexpected consequences. It is imperative, therefore, to recognize the significance of collective efforts in protecting CI. The complexity and magnitude of emerging threats exceed the capabilities of individual states, necessitating a collaborative approach among nations, international organizations, and other stakeholders. In this regard 16 March 2023, after the NATO-EU joint meeting, the " NATO-EU Task Force on Resilient Critical Infrastructure" announcement shows the importance that NATO attaches to collective security and resilience for CI effort with other stakeholders.

NATO, as a key player in ensuring collective security, has a vital role to play in protecting CI in the maritime environment. The alliance's commitment to building resilience, as demonstrated by its *Strengthened Resilience Commitment* in 2021, underscores its dedication to effectively carry out its core missions of collective defence, crisis management, and cooperative security. It should also be noted that to see the importance of CI in maritime environment for NATO, four of the twenty-eight centers of excellence accredited by NATO, including MARSEC COE, deal with maritime issues. In this direction leveraging its deterrent value, NATO not only possesses credible military capabilities but also works towards the protection of allies' CI during crises and proactive crisis management in the event of damage.

To enhance the protection and resilience of CI in the maritime environment, NATO and its allies should implement a series of key findings and recommendations. Experience sharing and joint decision-making among allies will facilitate the exchange of best practices and the development of unified strategies. Increased intelligence and information sharing will enhance situational awareness, enabling proactive responses to potential threats. The establishment of a comprehensive and mutually shared strategy based on Maritime Situational Awareness (MSA) will aid in identifying and managing risks to maritime critical infrastructure.

Harnessing technological advancements, such as the Defense Innovation Accelerator for the North Atlantic (DIANA) , will bolster the ability to detect, respond to, and recover from disruptive events affecting critical infrastructure. Moreover, a multi-stakeholder approach involving governments and the private sector is crucial in developing and implementing a comprehensive CISR policy that addresses cyber threats, maritime security challenges, energy security, and legal aspects impacting critical infrastructure.

Addressing the impact of cyberspace on critical infrastructures is of paramount importance, given the increasing reliance on digital systems and the sophistication of cyber threats. Similarly, the effects of climate change on critical infrastructures must be taken into account to ensure their security and resilience against environmental challenges. Emphasizing the legal foundations of multinational decision-making and implementation within NATO will foster effective and coordinated protection of critical infrastructures.

Furthermore, enhancing intelligence capabilities, conducting scenario-based studies, considering the impact of unmanned and autonomous systems on the protection of critical infrastructure and focusing on underwater communication systems are essential components of a comprehensive approach. By proactively addressing these areas, NATO and its allies can better understand and prepare for potential threats, thereby strengthening the overall resilience of critical infrastructure. At this point, the announcement of establishing a Critical Underwater Infrastructure Coordination Cell by NATO on 15 February 2023 is a new and significant development.

Finally, the protection of critical infrastructure in the maritime environment requires a collaborative and multidimensional effort. By implementing the recommended measures and focusing on key areas of concern, NATO and its allies can enhance the protection, security, and resilience of critical infrastructure, thus safeguarding societies, ensuring the continuity of essential services, and bolstering the overall security and stability of the alliance and the global system. The recognition that NATO is only as strong as its weakest link should serve as a constant reminder to prioritize the protection of critical infrastructure as an indispensable element of collective security.

(157)The establishment of DIANA was announced during the writing of the conclusion of this study paper and is therefore not mentioned in detail in the text.
(158)Like DIANA, the establishment of the Critical Submarine Infrastructure Coordination Cell post-dates the writing of this study paper and is only mentioned in the conclusion.

REFERENCES

Adetunji, Jo. 'Hijacked Saudi Oil Tanker Sirius Star on the Move'. The Guardian, 9 January 2009, sec. World news.
www.theguardian.com/world/2009/jan/09/somalia-pirates-supertanker-ransom

Ang, Yuen Yuen. 'Demystifying Belt and Road'. Foreign Affairs, 29 December 2022.
www.foreignaffairs.com/articles/china/2019-05-22/demystifying-belt-and-road

Bağbaşlıoğlu, Arif. 'NATO'nun Deniz Güvenliği Algısı: Süreklilik ve Değişim'. Güvenlik Bilimleri Dergisi 10, no. 1 (16 May 2021): 59–78.
https://doi.org/10.28956/gbd.843006

BBC News. 'What makes Russia's new spy ship Yantar special?' 3 January 2018, sec. Europe.
www.bbc.com/news/world-europe-42543712

Bearse, Ronald S. 'Introduction To Critical Infrastructure Security And Resilience (CISR)'. Presentation presented at the NATO COE-DAT CIP Onlinr Course, 11 November 2022.

Bıçakçı, Salih. 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'. Presentation presented at the MARSEC-COE Maritime Critical Infrastructure Protection Workshop, 10 December 2021.

Brown, K. Ann. Critical Path: A Brief History of Critical Infrastructure Protection in the United States. Critical Infrastructure Protection Project, George Mason University. United States of America, 2006.
https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_CriticalPath.pdf

'Brussels Summit Communiqué Issued by NATO Heads of State and Government (2021)'. NATO. Accessed 17 January 2023.
www.nato.int/cps/en/natohq/news_185000.htm

'Brussels Summit Declaration issued by NATO Heads of State and Government (2018)'. NATO. Accessed 9 January 2023.
www.nato.int/cps/en/natohq/official_texts_156624.htm

Bueger, Christian. 'Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU', n.d.

Burdette, Lane. 'Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy'. Journal of Public and International Affairs. Accessed 18 January 2023.
https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy

Çakır, Mustafa. 'Güvenliğin Dönüşümü ve Ulusal Güvenlik'. The Journal of Diplomacy and Strategy 3, no. 2 (2022).
https://dergipark.org.tr/en/download/article-file/2786023

Capacity Media. 'PCCW Global signs up to extend PEACE cable to southern Africa', 20 January 2020.
www.capacitymedia.com/article/29otbyvgrerkbxkdezmrk/news/pccw-global-signs-up-to-extend-peace-cable-to-southern-africa

Capria, Amerigo, Elisa Giusti, Christian Moscardini, Michele Conti, Dario Petri, Marco Martorella, and Fabrizio Berizzi. 'Multifunction Imaging Passive Radar for Harbour Protection and Navigation Safety'. IEEE Aerospace and Electronic Systems Magazine 32, no. 2 (February 2017): 30–38.
https://doi.org/10.1109/MAES.2017.160025

REFERENCES

Çelikpala, Mithat. 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'. Presented at the MARSEC-COE Maritime Critical Infrastructure Workshop, March 2022.

Çetikli, Deniz. 'Critical Infrastructure Protection on Maritime Environment'. Presentation, NATO MARSEC-COE, 5 December 2022.

'Chicago Summit Declaration issued by NATO Heads of State and Government (2012)'. NATO. Accessed 15 January 2023.
www.nato.int/cps/en/natohq/official_texts_87593.htm

'Cyber Intelligence in MSO'. Presented at the MARSEC COE Cyber Intelligence in MSO Concept Development Workshop, 5 April 2023.

Çetin, Oktay, and Mesut Köseoğlu. 'A Study on the Classification of Maritime Security Threat Topics'. International Journal of Environment and Geoinformatics 7, no. 3 (6 December 2020): 365–71.
https://doi.org/10.30897/ijegeo.742336

'COE-CSW - CENTRE OF EXCELLENCE for Operations in Confined and Shallow Waters: Another Milestone in Harbour Protection'. Accessed 18 January 2023.
www.coecsw.org/our-work/spotlights/archive/another-milestone-in-harbour-protection/

'Critical Infrastructure Facts Page'. Accessed 3 January 2023.
www.networkintegritysystems.com/critical-infrastructure

'Cyberspace In Deep Water: Protecting Undersea Communication Cables'. Accessed 16 January 2023.
https://www.belfercenter.org/sites/default/files/files/publication/PAE_final_draft_-_043010.pdf

Dalaklis, Dimitrios. 'Marine Energy Transport Infrastructure Conservation Challenges: Educated Predictions for the Future'. Presentation presented at the MARSEC-COE Maritime Critical Infrastructure Workshop, 30 March 2022.

David, Rona Rita. 'Submarine Cables: Risks and Security Threats'. Energy Industry Review (blog), 25 March 2022.
https://energyindustryreview.com/analysis/submarine-cables-risks-and-security-threats/

'Déclaration du Sommet de Bucarest publiée par les chefs d'État et de gouvernement des pays membres de l'OTAN (2008)'. NATO. Accessed 15 January 2023.
www.nato.int/cps/fr/natohq/official_texts_8443.htm

Defender Project. 'Defending the European Energy Infrastructures'. Europian Commission, 7 November 2017.
ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7096f83&appId=PPGMS

'Denizaltı Kablo Haritası'. Accessed 18 January 2023.
www.submarinecablemap.com/submarine-cable/peace-cable

Doğan, Diren. 'Türkiye'de Tayvan Çalışmaları - III'. In GRİ BÖLGE STRATEJİLERİ ÇERÇEVESİNDE TAYVAN'IN HİBRİT TEHDİTLERLE MÜCADELE STRATEJİSİ. Ankara Üniversitesi Yayınları, n.d.
http://apam.ankara.edu.tr/wp-content/uploads/sites/485/2022/07/Turkiyede-Tayvan-Calismalari-III.pdf.

'Emerging Threats to Maritime Energy Infrastructure'. NATO. Accessed 14 January 2023.
www.nato.int/cps/en/natohq/news_124544.htm.

REFERENCES

'Energy security'. NATO. Accessed 13 January 2023.
www.nato.int/cps/en/natohq/topics_49208.htm

Ertosun, Ferhat M. 'Harbor Protection as Part of CIP/CEIP (Critical Infrastructure&Critical Energy Infrastructure Protection)'. Presentation presented at the NATO MARSEC COE Maritime Critical Infrastructure Protection(MCIP) Workshop, 16 May 2022.

European Commission - European Commission. 'Critical Infrastructure Resilience: stronger rules'. Text. Accessed 12 January 2023.
https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6238

'European Commission SUCCESS Project Report'. Accessed 11 January 2023.
ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b7096f83&appId=PPGMS

European Marine Observation and Data Network (EMODnet). 'Map of the week – Submarine telecommunication cables', 23 August 2019.
https://emodnet.ec.europa.eu/en/map-week-%E2%80%93-submarine-telecommunication-cables

'European Security & Defence'. Accessed 18 January 2023.
https://euro-sd.com/wp-content/uploads/2021/04/ESD_02_2019_WEB-1.pdf

Evans, Carol V, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, et al. 'Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1)'. USAWC Press, November 2022.

'Ever Given: an Example of How Complex International Liability for Damages Can Be'. Accessed 14 January 2023.
www.ibanet.org/ever-given-international-liability-damages

'Factsheet: Submarine Cables – Maritime Awareness Project'. Accessed 16 January 2023.
https://map.nbr.org/2018/07/submarine-cables/

'From Fragmented Sea Surveillance to Coordinated Maritime Situational Awareness'. Accessed 6 January 2023.
www.marseccoe.org/wp-content/uploads/2022/01/MSA_Study_Paper.pdf

Gechkova, Teodora. 'Security of Marine Critical Infrastructure'. KNOWLEDGE - International Journal 49, no. 5 (15 December 2021): 945–49.

Gechkova, Teodora, and Tiana Kaleeva. 'Harbour Infrastructure Protection – PESTLE Analysis'. KNOWLEDGE - International Journal 49, no. 5 (15 December 2021): 961–67.

'Grid Resilience: Priorities for the Next Administration'. Accessed 12 January 2023.
https://gridresilience.org/wp-content/uploads/2020/11/NCGR-Report-2020-Full-v2.pdf

H. Lau, Constance, and Beverly Scott. 'Strengthening Regional Resilience: Final Report and Recommendations'. National Infrastructure Advisory Council Final Report and Recommendations, 21 November 2013.

Hasen, Hazar Strateji Enstitüsü. 'Kritik Enerji Altyapı Güvenliği El Kitabı'. Accessed 14 January 2023.
www.academia.edu/10027314/Kritik_Enerji_Altyap%C4%B1_G%C3%BCvenli%C4%9Fi_El_Kitab%C4%B1

Heijmans, Philip, Cindy Wang, and Samson Ellis. 'Taiwan tensions raise alarms over risks to world's subsea cables'. The Japan Times, 31 October 2022.
www.japantimes.co.jp/news/2022/10/31/asia-pacific/taiwan-tensions-subsea-cables/

REFERENCES

Hillman, Jonathan. 'Securing the Subsea Network A Primer for Policymakers'. The Center for Strategic and International Studies (CSIS), March 2021.
https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ

webarchive.nationalarchives.gov.uk/eu-exit/https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114

'Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance)'. Text. Queen's Printer of Acts of Parliament. Accessed 3 January 2023.
www.legislation.gov.uk/eudr/2008/114/article/2

'ICPC International Call to Action for COVID-19', 6 April 2020.
https://subtelforum.com/icpc-international-call-to-action-for-covid-19/

IEA. 'Energy Security – Topics'. Accessed 11 January 2023.
www.iea.org/topics/energy-security

IEA. 'Net Zero by 2050 – Analysis'. Accessed 14 January 2023.
www.iea.org/reports/net-zero-by-2050

IEA. 'Pathway to critical and formidable goal of net-zero emissions by 2050 is narrow but brings huge benefits, according to IEA special report - News'. Accessed 13 January 2023.
www.iea.org/news/pathway-to-critical-and-formidable-goal-of-net-zero-emissions-by-2050-is-narrow-but-brings-huge-benefits

IEA. 'WEO-2018 Special Report: Offshore Energy Outlook – Analysis'. Accessed 9 January 2023.
www.iea.org/reports/offshore-energy-outlook-2018

IISS. 'The Digital Silk Road: Introduction'. Accessed 18 January 2023.
www.iiss.org/blogs/analysis/2022/12/digital-silk-road-introduction

'Invisible and Vital: Undersea Cables and Transatlantic Security'. Accessed 16 January 2023.
www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

'İsveç'ten Kuzey Akım 1 ve Kuzey Akım 2 Gaz Sızıntılarında Ağır Sabotaj Tespiti'. Accessed 17 January 2023.
www.aa.com.tr/tr/dunya/isvecten-kuzey-akim-1-ve-kuzey-akim-2-gaz-sizintilarinda-agir-sabotaj-tespiti/2742068

Jamestown. 'Beijing's Growing Influence on the Global Undersea Cable Network'. Accessed 18 January 2023.
https://jamestown.org/program/beijings-growing-influence-on-the-global-undersea-cable-network/

Karabacak, Bilge. 'USAK Kritik Altyapı Güvenliği Projesi Sonuç Raporu'. Accessed 13 January 2023.
www.academia.edu/21583796/USAK_Kritik_Altyap%C4%B1_G%C3%BCvenli%C4%9Fi_Projesi_Sonu%C3%A7_Raporu

Kayser, Sümer. 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'. Presentation presented at the MARSEC-COE Maritime Critical Infrastructure Protection Workshop, 10 December 2021.

Kharpal, Arjun. 'Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice'. CNBC. Accessed 18 January 2023.
www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

REFERENCES

Kim, Jonathan. 'Submarine Cables: the Invisible Fiber Link Enabling the Internet'. Dgtl Infra (blog), 5 May 2022.
https://dgtlinfra.com/submarine-cables-fiber-link-internet/

Kozanhan, M. Kağan, and İbrahim Bayezit. 'Terrorist Threat with Improvised Explosive Device (IED) in the Marine Environment and Its Effects on Maritime Security'. Güvenlik Stratejileri 16, no. 34 (2020).
https://doi.org/10.17752/guvenlikstrtj.768616

Lawfare. 'Cutting the Cord: The Legal Regime Protecting Undersea Cables', 21 November 2017.
www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables

Lawfare. 'Evaluating the Russian Threat to Undersea Cables', 5 March 2018.
www.lawfareblog.com/evaluating-russian-threat-undersea-cables

'LESSONS FROM THE MUMBAI TERRORIST ATTACKS'. Accessed 21 January 2023.
www.govinfo.gov/content/pkg/CHRG-111shrg49484/html/CHRG-111shrg49484.htm

Lu, Marcus. 'Ranked: The World's Largest Container Shipping Companies'. Visual Capitalist, 26 July 2022.
www.visualcapitalist.com/worlds-largest-container-shipping-companies-2022/

M. Akar, Müge, Aslıhan A. Kemer, and Murat Jane. 'Good Practices in Counter Terrorism in Maritime Domain'. Seminar Report. Istanbul, Türkiye: Centre of Excellence Defence Against Terrorism (COE-DAT), 11 October 2022.

'Maritime Trade: Embracing the Ocean: Delivering the Trade Benefits of the National Shipbuilding Strategy Refresh', n.d.

Mauldin, Alan. 'Cable Breakage: When and How Cables Go Down'. Accessed 16 January 2023.
https://blog.telegeography.com/what-happens-when-submarine-cables-break

'The Criticality of Submarine Telecommunications Cables'. Presented at the Maritime Critical Infrastructure Protection Workshop, NATO MARSEC COE, 30 March 2022.

mc.nato.int. 'Operation OCEAN SHIELD'. Accessed 15 January 2023.
https://mc.nato.int/missions/operation-ocean-shield.aspx

Media, Fresh. 'Legal information | NATO Energy Security Centre of Excellence'. Legal information | NATO Energy Security Centre of Excellence. Accessed 15 January 2023.
https://enseccoe.org/en/legal-information/352

NATO. 'Alliance Maritime Strategy'. NATO. Accessed 6 January 2023.
www.nato.int/cps/en/natohq/official_texts_75615.htm

'Allied Joint Force Command Norfolk declares Full Operational Capability'. NATO. Accessed 17 January 2023.
www.nato.int/cps/en/natohq/news_185870.htm

'Madrid Summit Declaration Issued by NATO Heads of State and Government (2022)'. NATO. Accessed 15 January 2023.
www.nato.int/cps/en/natohq/official_texts_196951.htm

'NATO Stands up Undersea Infrastructure Coordination Cell'. NATO. Accessed 16 May 2023.
www.nato.int/cps/en/natohq/news_211919.htm.

REFERENCES

'Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers'. NATO. Accessed 17 January 2023.
www.nato.int/cps/en/natohq/opinions_178946.htm

'Operation Active Endeavour (2001-2016)'. NATO. Accessed 15 January 2023.
www.nato.int/cps/en/natohq/topics_7932.htm

'Operation Sea Guardian'. NATO. Accessed 15 January 2023.
www.nato.int/cps/en/natohq/topics_136233.htm

'**NATO 2022 Strategic Concept'. Accessed 3 January 2023.**
www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

'NATO 2030: United for New Era'. Accessed 3 January 2023.
www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO Maritime Security Centre of Excellence (MARSEC-COE). 'MARSEC-COE Enlargement Brochure', 2022.
www.marseccoe.org/published-work/#single/0

NATO Review. 'NATO DERGİSİ - Hibrit savaş döneminde enerji güvenliği', 13 January 2021.
www.nato.int/docu/review/tr/articles/2021/01/13/hibrit-savas-doeneminde-enerji-guevenligi/index.html

NATO Review. 'NATO Review - Energy security: a critical concern for Allies and partners', 26 July 2018.
www.nato.int/docu/review/articles/2018/07/26/energy-security-a-critical-concern-for-allies-and-partners/index.html

NATO Review. 'NATO Review - Energy Security in the Era of Hybrid Warfare', 13 January 2021.
www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html

'NATO Strategic Concept 2010'. Accessed 15 January 2023.
www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

Nordenman, Magnus. 'The Naval Alliance: Preparing NATO for a Maritime Century'. Atlantic Council, June 2015.
www.atlanticcouncil.org/in-depth-research-reports/report/the-naval-alliance-preparing-nato-for-a-maritime-century

Öğütçü, Caner. 'MARSEC-COE Maritime Critical Infrastructure Protection Workshop'. Presented at the MARSEC-COE Maritime Critical Infrastructure Protection Workshop, 10 December 2021.

Özker, Uğur. 'Türkiye'de Kritik Altyapı ve Siber Güvenlik'. Konrad-Adenauer-Stiftung Türkiye, November 2022.
www.kas.de/documents/283907/283956/KAS+x+EDAM_%C3%96zker_T%C3%BCrkiye%27de+Kritik+Altyap%C4%B1+ve+Siber+G%C3%BCvenlik.pdf/d9da96b2-8bdf-36d3-96d9-012b929c9a88?version=1.1&t=1669892363991

"Protection of Maritime Transportation Infrastructure"(Pipelines, LNG Routes and Subsea Cables)'. Presented at the Maritime Critical Infrastructure Protection(MCIP) Workshop, NATO MARSEC COE, 30 March 2022.

Ralby, Ian, and Bochman. 'Cybersecurity concerns for the energy sector in the maritime domain'. Atlantic Council (blog), 6 December 2021.
www.atlanticcouncil.org/in-depth-research-reports/issue-brief/cybersecurity-concerns-for-the-energy-sector-in-the-maritime-domain/

REFERENCES

Ratiu, Andrea. 'Cyber defense across the ocean floor: The geopolitics of submarine cable security'. Atlantic Council (blog), 13 September 2021.
www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/

Reconnecting Asia. 'Mapping China's Digital Silk Road', 19 October 2021.
https://reconasia.csis.org/mapping-chinas-digital-silk-road/

'Review of Maritime Transport 2020'. REVIEW OF MARITIME TRANSPORT, 2020.
Salerno-Garthwaite, Andrew. 'Seabed warfare is a "real and present threat"'. Naval Technology (blog), 20 December 2022.
www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/

'Riga Summit Declaration Issued by NATO Heads of State and Government (2006)'. NATO. Accessed 15 January 2023.
www.nato.int/cps/en/natohq/official_texts_37920.htm

Sanger, David E., and Eric Schmitt. 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort'. The New York Times, 25 October 2015, sec. World.
www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html

Schadlow, Nadia. 'Protecting Undersea Cables Must Be Made a National Security Priority'. Accessed 18 January 2023.
www.hudson.org/national-security-defense/protecting-undersea-cables-must-be-made-a-national-security-priority

'Securing Asia's Subsea Network: U.S. Interests and Strategic Options'. Accessed 17 January 2023.
www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options

'Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU', n.d.

services, WJI staff and wire. 'Rebranded Huawei Marine Networks to supply the cable for Asia Link Cable System'. Accessed 18 January 2023.
www.wirenet.org/news-categories/item/855-rebranded-huawei-marine-networks-to-supply-the-cable-for-asia-link-cable-system

SIM, Susan. 'Port Security'. Presented at the Good Practices in Counter Terrorism in Maritime Domain, 11 October 2022.

South China Morning Post. 'China builds undersea cable bases amid digital infrastructure rivalry', 12 December 2021.
www.scmp.com/news/china/diplomacy/article/3159328/china-builds-undersea-cable-bases-amid-digital-infrastructure

South China Morning Post. 'Next battleground in US-China tech war: undersea internet cables', 14 December 2019.
www.scmp.com/week-asia/politics/article/3042058/us-china-tech-wars-new-battleground-undersea-internet-cables

'Strategic Importance of, and Dependence on, Undersea Cables'. Accessed 17 January 2023.
https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf

'Submarine Cable Map'. Accessed 16 January 2023.
www.submarinecablemap.com/

Sutton, H. I. 'Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables'. Naval News (blog), 19 August 2021.
www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/

REFERENCES

TeleGeography. 'Submarine Cable FAQs'. Accessed 16 January 2023.
www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

'The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices'. Accessed 4 January 2023.
www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

'The Role and Relevance of the Maritime Domain in an Urban-Centric Operational Environment'. Accessed 18 January 2023.
www.coecsw.org/fileadmin/content_uploads/projects/Role_and_Relevance_of_the_Maritime_Domain_in_an_Urban-Centric_Operational_Environment.pdf

Tunca, H. Ömer. 'Defence Industry Infrastructure Protection from Terorrist Attacks: Turkish Experience'. Presentation presented at the Critical Infrastructure Protection from Terrorist Attacks Course, COE-DAT, n.d.

Venckunas, Audrius. 'Harbour Protection Doctrine'. Presented at the NATO MARSEC COE Maritime Critical Infrastructure Protection(MCIP) Workshop, 11 May 2022.

WANG, Christoph NEDOPIL. 'Kuşak ve Yol Girişimi Ülkeleri (BRI) – Yeşil Finans ve Kalkınma Merkezi'. Accessed 18 January 2023.
https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/

'Wales Summit Declaration issued by NATO Heads of State and Government (2014)'. NATO. Accessed 15 January 2023.
www.nato.int/cps/en/natohq/official_texts_112964.htm

Watts, Robert B. 'Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment'. Homeland Security Affairs 1, no. 2 (2005).
https://apps.dtic.mil/sti/pdfs/ADA484165.pdf

'While Oceans Cover 70 Per Cent of Earth's Surface, Understanding Has Lagged, Speakers in Lisbon Dialogue Stress, Offering Ways to Close Knowledge Gap | UN Press'. Accessed 6 January 2023.
https://press.un.org/en/2022/sea2152.doc.htm

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

NOTES

MARITIME SECURITY CENTRE OF EXCELLENCE

''Working Together for Maritime Security''