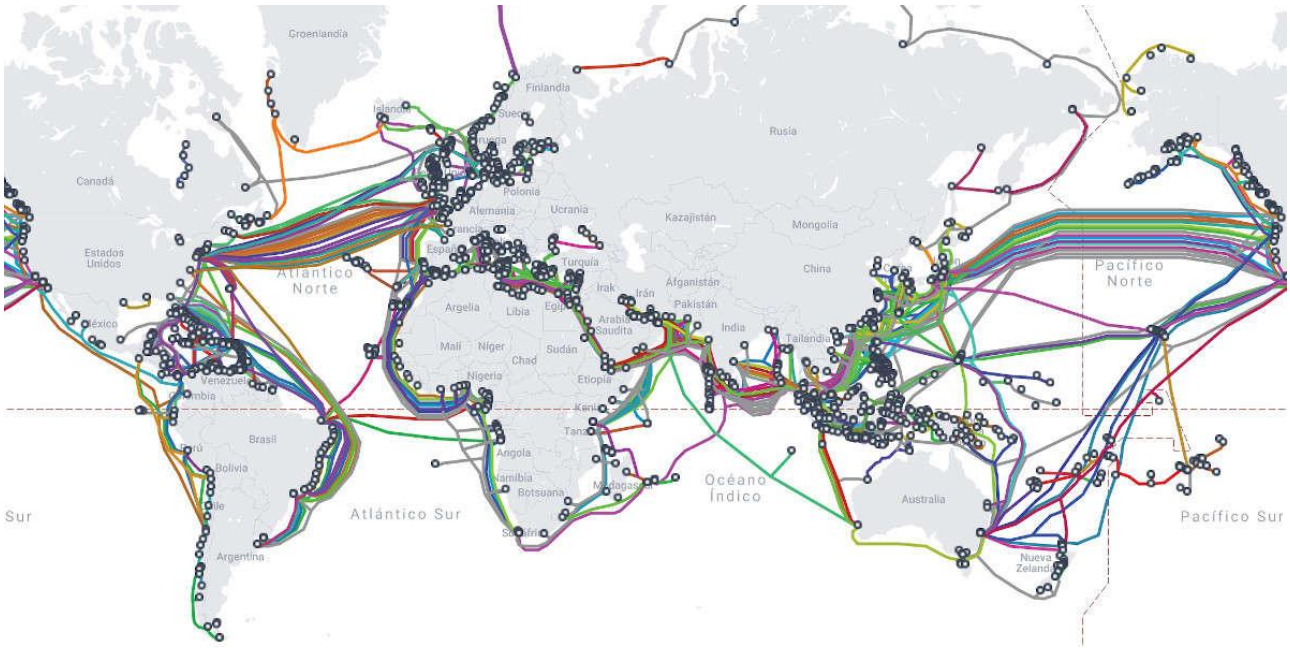
Naval Mine Warfare Centre of Excellence

Critical Undersea Infrastructure (CUI)



Ostend 2026

Author: CDR Rutger van der Werff (RNLN), MSc.
Branch Head Concept Development and Experimentation
NMW-COE@mil.be

The figure on the front page: Undersea cables' vulnerability: A hidden network of vital connectivity. Gonzalo Vázquez Orbaiceta, Universidad de Navara, 08/03/2023.

DISCLAIMER:
This document is a product of the Naval Mine Warfare Centre of Excellence (NMW COE) and initiated by this Centre, with the knowledge that there are still a lot of unanswered questions related to this topic. It does not necessarily reflect the views of the North Atlantic Treaty Organization (NATO), or the Framework/Sponsoring Nations of NMW COE.

COPYRIGHT:
This document is under the copyright law; portions of the document may be quoted or reproduced without permission, provided a standard credit is included. Any comprehensive reproduction requires prior written permission of the NMW COE

1 Contents

EXECUTIVE SUMMARY 4

1 CHAPTER I: INTRODUCTION 6

1.1 General 6

1.2 Aim 6

1.3 Definitions 7

1.4 Methodology 7

2 CHAPTER II – History and status of CUI 8

2.1 History of CUI 8

2.2 Status of CUI 8

3 Threats to CUI and consequences 10

3.1 Introduction 10

3.2 Threats to cables 11

3.3 Threats to pipelines: 12

3.4 Consequences: 12

4 CHAPTER IV: Legal implications and operational challenges regarding the protection of CUI 13

4.1 Legal implications 13

4.2 Operational challenges 14

5 CHAPTER V – Solutions for enhancing the protection of CUI. 16

5.1 Operational solutions 17

5.2 Common procedure and doctrine 18

6 Case Study 21

7 CHAPTER VI- Conclusion 24

ANNEX ALFA - List of abbreviations. 27

ANNEX BRAVO - Bibliography 28

EXECUTIVE SUMMARY

This paper examines the growing challenge of protecting Critical Undersea Infrastructure (CUI), including submarine cables and pipelines that are essential to global communications, energy distribution, and economic stability. It analyses the threats facing these assets, the legal and operational difficulties involved in their protection, and the feasibility of developing common doctrines and procedures for safeguarding them.

CUI faces a wide range of threats. Accidental risks include fishing activities, ship anchors, severe weather, geological events, corrosion, aging systems, and maintenance failures. More concerning is the rise of deliberate threats such as sabotage, espionage, and hybrid warfare conducted by state and non-state actors using civilian vessels, divers, submarines, and remotely operated systems. Damage to these networks can cause major disruptions to telecommunications, energy security, trade, and national economies, making their protection a strategic priority.

Legal challenges complicate protection efforts. The principle of freedom of navigation on the high seas limits preventive measures against suspicious vessels. Jurisdictional issues create accountability gaps, as responsibility for investigating and prosecuting incidents generally lies with either the flag state of the vessel or the perpetrator's state of citizenship. Furthermore, under the law of armed conflict, some forms of CUI may be considered legitimate military targets during wartime. Operationally, authorities must determine which infrastructure assets deserve priority protection, monitor vast maritime areas, and develop specialized expertise to identify and respond to acts of sabotage.

Effective protection begins with a comprehensive inventory of infrastructure and a risk-based assessment of criticality and vulnerability. This enables efficient allocation of security resources. Operational measures include increased naval and coast guard patrols, supported by unmanned underwater vehicles (UUVs) equipped with cameras, sonar, magnetometers, and artificial intelligence for inspection, mapping, and threat detection. Additional resilience can be achieved through integrated sensor systems, seabed monitoring networks, intrusion detection capabilities, and rapid-response forces using surface vessels, aircraft, remotely operated vehicles (ROVs), and specialized divers. Redundancy through multiple cables, pipelines, and interconnections, combined with robust repair capabilities, reduces the impact of disruptions.

The study finds that a common doctrine for CUI protection is increasingly feasible because allies share a common perception of vulnerability. A federated protection model would include a shared threat assessment, standardized operational procedures, trusted information-sharing networks, and common cybersecurity and resilience standards. A

lifecycle protection approach should integrate security from design and deployment through monitoring and recovery.

Evidence of such a doctrine is already emerging. NATO has established the Critical Undersea Infrastructure Coordination Cell and related operational structures, while operations such as Baltic Sentry demonstrate practical implementation. The European Union has introduced the Cable Security Action Plan and Cable Security Toolbox to enhance prevention, detection, response, resilience, and cooperation among member states, NATO, industry, and international partners. Existing ISO subsea and pipeline standards provide a strong technical foundation.

Case Study: the December 2024 EstLink 2 cable disruption between Estonia and Finland illustrates these challenges. Damage, likely caused by a dragging ship anchor, disrupted a critical electricity link and required electricity rerouting, local generation support, extensive investigations, and specialized repair operations. The incident highlighted the importance of physical protection, monitoring, redundancy, emergency coordination, and long-term investment in resilient energy systems. Overall, the study concludes that coordinated international action, common procedures, advanced monitoring technologies, and resilience-focused planning are essential to securing critical undersea infrastructure against evolving threats

1 CHAPTER I: INTRODUCTION

1.1 General

Subsea infrastructures, such as high-speed data cables, electricity connectors/ cables and underwater pipelines, are critical for our modern way of life. Underwater electricity connectors and cables are essential for transmitting power between offshore energy assets, islands, and mainland grids, enabling reliable electricity delivery where overhead power lines are not feasible (Research and Markets, 2026) Subsea data cables provide essential connection to the internet worldwide, while pipelines power entire nations with energy. With the attacks on the Nord Stream pipelines in mind, these kinds of infrastructure are targeted more frequent with acts that do not amount to an armed attack on a state's sovereignty although being disruptive for the economy or security of that State (Halog et all, 2023, p.1).

Vulnerability of CUI has recently been brought to the forefront. Incidents with the Baltic connector pipeline (2023), the incidents with communications cable C-Lion1 between Finland and Germany, the BCS East-West Interlink data cable between Sweden and Lithuania and ESTLINK 2/ data cable disruptions between Finland and Estonia/ Germany (2024) (see case study), highlight the risk of deliberate damage to CUI across Europe. It follows the Nord Stream pipeline explosions, also bearing the hallmarks of sabotage (Monaghan et all, 2023, p.1). But the list of incidents related to undersea cables is more extensive than that. If you look at the last 5 years there are nine incidents, not only sabotage, proving the vulnerability of undersea cables (Lott, 2024, p.2).

These examples underline the importance of intensified efforts to improve the protection of critical undersea infrastructure. It's obvious that the owners of the cables and pipelines have the responsibility to implement necessary protective measures, but it must also be clear that the security of this infrastructure should be a NATO priority. The protection of CUI includes robust coordination, to actively monitor and counter malign or hybrid threats, denying any aggressor the cover of "plausible deniability" (NATO media Centre, 2024, article p.1)

This study project has been initiated by the Italian Navy. It will be presented to Allied Command Transformation (ACT) as part of concept development work for 2026.

1.2 Aim

The aim of this study project is to examine the role of Naval Mine Warfare (NMW) in the protection of Critical Undersea Infrastructure (CUI) and in supporting seabed operations. The project assesses current threat perceptions and explores the legal and operational implications related to the protection of CUI. In addition, it investigates the feasibility of developing a common procedure and doctrine for CUI protection and seabed operations. To

support its findings, the study includes a case study that illustrates practical applications and challenges.

1.3 Definitions

To avoid misunderstanding, the following definition for CUI is used: A global network of undersea data cables, electricity connectors and pipelines supplying oil and gas (necessary to maintain normalcy in daily life). (NATO review, 2024, article p.1) One can argue that stationary equipment for scientific research does also belong to that list.

1.4 Methodology

The author used three different sources: First, publications from respected authors in the field of protection of CUI (see bibliography). Besides that, information was gathered during the Operational Maritime Law conference in Ljubljana in September 2024. Finally, the author used the knowledge about the protection of CUI gained during his time working within the NMW community.

2 CHAPTER II – History and status of CUI

2.1 History of CUI

The submarine cable industry has been installing infrastructure on the seafloor since 1851, when the first submarine telegraph line was laid between England and France (MAOA, 2024). The first permanently transatlantic telegraph cable was laid in 1866. The first transatlantic telephone cable, from Scotland to Newfoundland was laid in 1956. The first underwater pipeline, for transporting oil from England to France was constructed in 1944 as part of the 'Pipeline under the Ocean'- project (Hopkins, 2007, p.11)

2.2 Status of CUI

There are roughly 600 undersea cables that connect the world, totalling about 900,000 miles (TeleGeography, 2024, FAQ). These cables use fibre- optic technology and are in most cases not wider than a fire hose. Most of these cables lie on the seabed floor, but nearer to the shore cables are buried under the seabed for protection.

Cables were traditionally owned by telecom carriers who would form a consortium of all parties interested in using the cable. In the late 1990s, an influx of entrepreneurial companies built lots of private cables and sold off the capacity to users. Both the consortium and private cable models still exist today, but one of the biggest changes in the past few years is the type of companies involved in building cables. Content providers such as Google, Meta, Microsoft, and Amazon are major investors in new cables. The amount of capacity deployed by private network operators – like these content providers – has outpaced internet backbone operators in recent years. Faced with the prospect of ongoing massive bandwidth growth, owning new submarine cables makes sense for these companies. (TeleGeography, 2024, FAQ).

Underwater electricity connectors and cables, commonly referred to as subsea power connectors and submarine power cables, are becoming critical infrastructure for the global energy transition. Worldwide deployment is accelerating due to rapid growth in offshore wind farms, cross-border grid interconnectors, island electrification projects, and offshore oil and gas electrification. High Voltage Direct Current (HVDC) submarine cables are increasingly favoured for long-distance transmission because they reduce transmission losses, while advanced wet-mate and dry-mate subsea connectors enable reliable underwater connection, maintenance, and expansion of offshore energy assets. Europe currently leads the sector due to extensive offshore wind development and international interconnector projects, while Asia-Pacific is experiencing the fastest growth as countries expand offshore renewable energy capacity and grid connectivity. Industry demand is also driving investment in larger cable-laying vessels and next-generation high-voltage cable technologies capable of transmitting more power over longer distances. (Research and Markets, 2026)

Submarine pipelines are utilised for the transport of water, bulk oil and gas products, and effluent, and they are usually manufactured from steel or high-density polyethylene. Submarine pipeline is the fastest, safest, and most economical and reliable means of transporting oil and gas continuously (Fang and Duan, 2014, p.1). Seventy percent of the world's crude oil and petroleum products run through submarine pipelines. Across the North Sea alone, there are 8000 kms of oil and gas pipelines (MARCOM presentation, OML conference, page 6). The longest oil/gas pipeline is/was the well- known Nord Stream pipeline (1224 km) in the Baltic Sea, designed to transport Russian natural gas to Europe. This twin subsea pipelines could transport 55 billion cubic metres of gas a year. The 1,166km Langeled gas pipeline runs under the North Sea (Norway to the UK), transporting 29 billion cubic meters of gas per year. The Ichthys Export Pipeline (Timor Sea), transports gas to Darwin in Australia. There are 365 billion cubic meters of natural gas present in that field (Offshore technology, 2014, whole page). To compare: the gas consumption in 2015 in Germany, Great Britain, Italy and France were 79,9/71,8/66,2/41,5 billion cubic meters respectively (Eurogas, 2015). These examples highlight the importance of undersea pipelines for the world's economy.

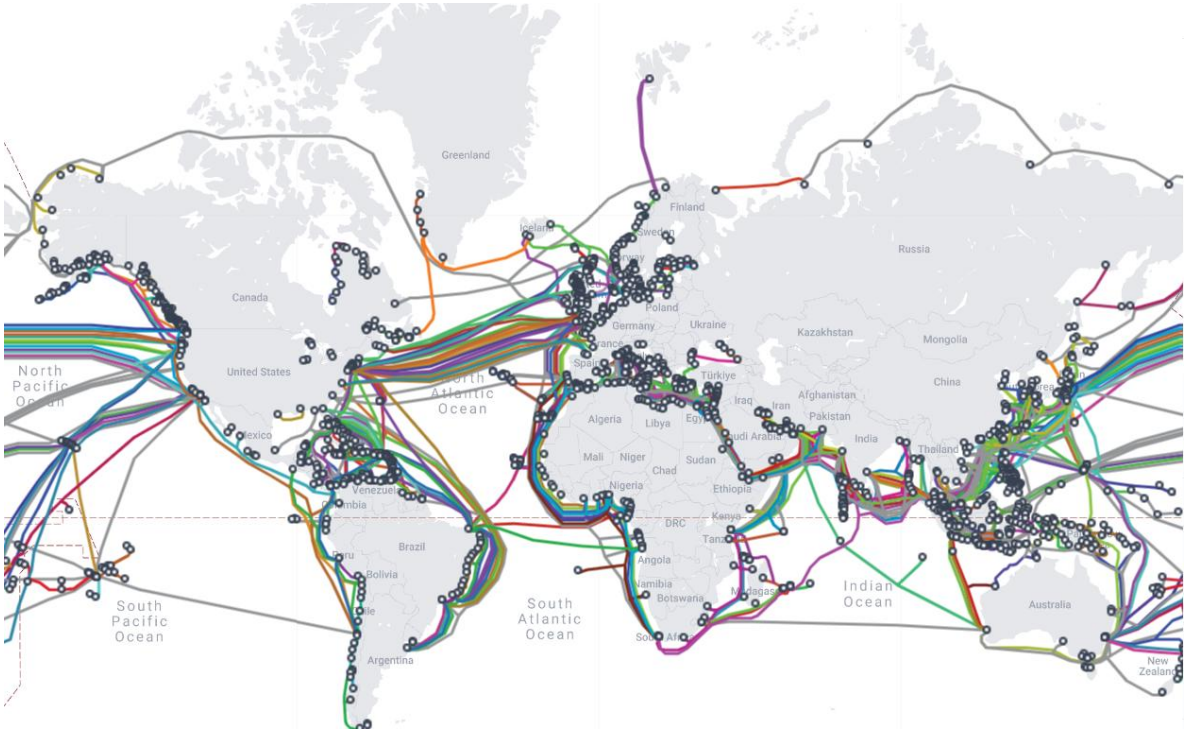


Fig. 2. Overview of the world's submarine cables 2024. Source: TeleGeography

We are looking at protecting these cables and pipelines: but against who or what? What are the threats? This will be the focus of the next chapter

3 Threats to CUI and consequences

3.1 Introduction

The demand for submarine cables will increase rapidly in the coming years due to the growing demand for data, fuelled by the expansion of cloud services and artificial intelligence. Furthermore, the shift to more sustainable energy sources, such as wind and solar power, will require more submarine connections to transport energy from offshore parks to the mainland (Lightbox, 2024, L. 32-36). Western intelligence agencies, politicians, think-tanks, and experts, have declared often that there is an existential risk to critical (undersea) infrastructure posed by state sabotage (Westley, 2024, L. 59-63).

Considering this existential risk, it is important to introduce the Russian Federation's efforts to expand its capabilities for underwater reconnaissance, intelligence collection, data acquisition, and potential sabotage operations. Russia's Main Directorate of Deep-Sea Research (GUGI) (Russian: Glavnoye Upravleniye Glubokovodnykh Issledovaniy) is a highly secretive organization within the Russian Ministry of Defence responsible for deep-sea operations, and underwater intelligence collection. GUGI operates a small but highly specialized fleet of intelligence vessels, special-purpose submarines, deep-diving nuclear submersibles, remotely operated vehicles (ROVs), and unmanned underwater systems designed for deep-sea operations and seabed access. Many of these assets can operate at depths far beyond those of conventional military submarines. Key platforms are:

- Yantar: An oceanographic research vessel frequently observed near undersea cable routes.
- Losharik: A nuclear-powered deep-diving special-purpose submarine capable of operating at extreme depths.
- Belgorod: A special-purpose submarine designed to support deep-sea missions and deploy autonomous underwater systems.

From a NATO perspective, GUGI represents a strategic capability that could be used to monitor, exploit, or potentially disrupt critical underwater infrastructure during a crisis or conflict. As a result, the protection of subsea cables, pipelines, and power interconnectors has become an increasing focus for NATO and European nations

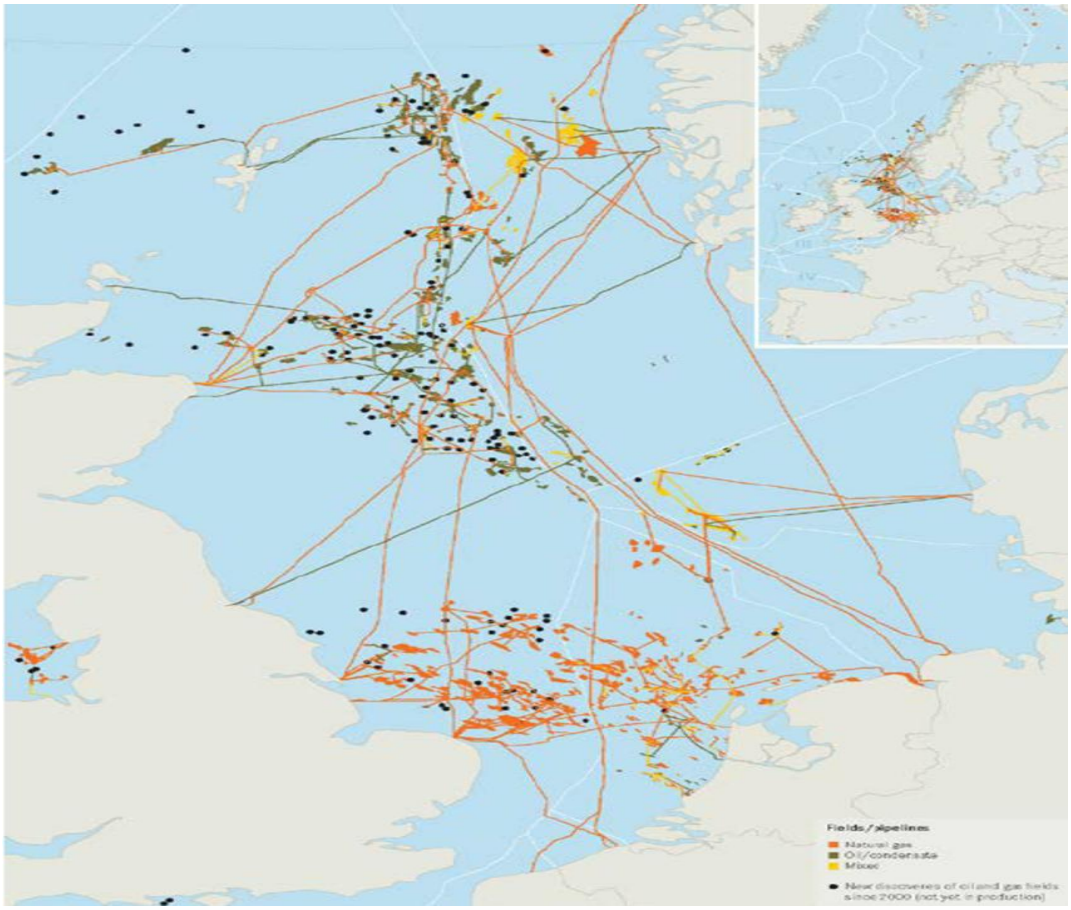


Fig 3. Map of offshore oil and gas pipelines in the North Sea (Source: Research Gate)

3.2 Threats to cables

Undersea cables can be highly vulnerable to a variety of factors. Most cable damage is unintentional, mainly stemming from accidental human interaction with the cables. Still, potential hazards to the cables range from anchoring and fishing equipment to extreme weather, and tectonic activity such as earthquakes and landslides. Damage to undersea cables is relatively common—an estimated 100 to 150 cables are severed each year—mostly from fishing equipment or anchors (Runde et all, 2024, L-54-58). Besides that, even marine life (sharks) has been seen to severely damage undersea cables.

Next to these unintentional ways of damaging cables there's an increase in the intentional damaging of cables and acts of espionage (gathering intel). With this we see a shift from non-state to state actors (Petrig, 2024, opening remarks). To carry out these acts of sabotage or damaging CUI, a variety of assets is used ranging from scuba divers, subsurface military assets (e.g. remotely operated vehicles), and deep-water submersibles, originally meant for commercial or scientific purposes to civilian ships.

3.3 Threats to pipelines:

As with submarine cables, submarine pipelines can be damaged unintentionally. Corrosion, caused by the chemical composition of compressed gas and water, hydraulic seal failure, pressure and temperature deviations increase hazards of pipeline rupture (Akhmetkaliyeva, 2020, L.17-19). Besides that, a worldwide aging pipeline infrastructure, a lack of proper maintenance, and even the type of materiel used impact the likelihood that a rupture could occur. Submarine landslides are potential risks because they can generate damaging tsunamis, severely damaging infrastructure such as offshore oil rigs and pipelines (Kappel, 2015, L.27-31).

When we look at intentional damaging of pipelines, we can tell that recent reports give us some ideas of the modus operandi in sabotage. Such attacks can happen in various ways, such as submarines and unmanned vehicles, fishing or sailing vessels with scuba divers on board hiding in everyday traffic or even ships anchoring intentionally in those areas (Kostoudis, 2023, L. 13-16).

3.4 Consequences:

In a squeezed global gas market, even relatively small upsets can send investors into a tizzy, sending prices higher. As an example: future prices for Europe's benchmark gas contract jumped 15% on Monday following Gasgrid's announcement that it had shut the Baltic Connector. Besides the inflation impact caused by shortages also supply security and/or the idea of not being able to get gas will impact human behaviour. The European [gas] market remains very tight, and any news is having an impact (Cooban, 2023, L.58-70). Any attack on a single connection in the networks that brings fuel, power, and data to our shores would likely have a relatively limited impact. However, a coordinated disruption to critical nodes and hubs could lead to cascading impacts which could affect entire systems and lead to spiralling costs of disruption, with knock-on effects across the wider economy as well as government functions, hospitals, and services. This could be a prelude to wider military action, or a hostile attempt to coerce a target state short of war (van Soest and Fine, 2024, L.81-87).

Before we turn to possible solutions to mitigate risks, we would like to highlight some of the challenges related to (the protection) of CUI.

4 CHAPTER IV: Legal implications and operational challenges regarding the protection of CUI

4.1 Legal implications

There are multiple legal implications surrounding the protection of CUI. This chapter will highlight the most important ones.

Before explaining the first one, we discuss two important treaties from the perspective of international law. The first is the Convention for the Protection of Submarine Telegraph Cables (1884 Cable Convention). Article II of this convention criminalizes intentional or negligent damage to submarine cables that could disrupt telegraphic communication. Article X permits any signatory nation's warship to inspect vessels suspected of damaging submarine cables in violation of the convention. The second treaty is the 1982 United Nations Convention on the Law of the Sea (UNCLOS). UNCLOS article 113 states that: "every state shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence."

The first implication is that these international treaties often lack mandatory power to enforce the said legal framework. There are no explicit provisions in these conventions in the maritime domain for use of force in CUI protection. The use of force remains linked to the right of self-defence. There is a lack of power to visit, board or seize. Closely related to this is the rule that states that: high seas are open to all states, comprising amongst other things the freedom of navigation. And because no state is allowed to subject any part of the high seas to its sovereignty, it's making it impossible to control these seas. Besides that, given the increasing importance of digital technology applications, the level of protection envisioned at the time these treaties were drafted is no longer sufficient. For example: UNCLOS is silent on intelligence gathering activities (MARCOM presentation, OML, page 24).

The second implication is how to (correctly) discipline the offender: If cables are wilfully or accidentally damaged by a ship or person, the jurisdiction to determine an appropriate punishment for the perpetrator lies with the state under whose flag the ship operates or that of the person's citizenship. Because this places onus on the perpetrator's state, not the state that owns the cable, there is no effective regime to ensure that the responsible party is held accountable directly (Paik and Counter, 2024, L. 71-76). Under international law, jurisdiction often rests primarily with the flag state, meaning an effective prosecution may depend on the willingness and capability of a state with little connection to the incident (Hartmann and Lott, 2025). Besides that, because of the geographical 'nature' of the challenge, it will in most cases

be very hard to attribute any action. Deniability is very easy to preserve. And even if the offender is seen committing the act, who will be the one(s) to react? In a countries TTW it looks quite clear who will respond, because if an incident or violation affecting underwater infrastructure occurs within a coastal state's maritime zone, the coastal state is generally responsible for exercising jurisdiction and enforcing its laws, and for investigating incidents and collecting evidence. But what about international waters? Will it be the country where the shareholders come from, will it be the country where the company is registered or will it be the importing/exporting countries of the energy? After all: cables don't (really) have flags.

A third implication is that critical underwater infrastructure can be seen as an *easy* lawful military target in wartime. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage (San Remo manual, 1994). What if the sabotage of a pipeline is seen as something that will give a definite military advantage. After all, no income from exporting gas makes it harder to continue fighting a war.

A fourth implication is that we are dealing with national interests, different domestic legal frameworks, varying risk perceptions between countries and a lack of a central cable registry to begin jurisdiction (MARCOM OML, 2024, page 25).

4.2 Operational challenges

First, which vital infrastructure does one specifically want to protect? An important question, that needs to be answered, when you want to respond quickly in the best possible way. Although there are initiatives undertaken to categorize and protect infrastructure, e.g. the EU directive NIS2, the cybersecurity law designed to improve the resilience and security of critical and important organizations across the EU (e.g. energy), there is no (real) prioritization made amongst different nations/industry where to aim at for physical protection. Besides that, who would be responsible for which part of international waters? A question not (yet) answered.

Second, even when there has been some prioritization, there is the geographic scope of the necessary protection. The distances to cover are huge. As of 2024, an estimated 600 submarine cables are present globally, adding up to 900.000 miles of submarine cables in service. Besides that, there are 20.000 miles of underwater oil and gas pipelines. As already mentioned, it's difficult for humans to affect infrastructure below 1000 meters of water depth, so not all the 920.000 miles can be seen as suitable for possible attacks, but the infrastructure within the Baltic Sea, North Sea and large parts of the Mediterranean Sea is. When we then look at area (distance) from a Naval Mine Counter Measures- perspective: our assets can approximately cover 24 nautical miles per day, per system (using the detect to engage cycle).

Third, operators, within NATO, are not trained to look for acts of sabotage. How to differentiate between legitimate and illegal activities? Is the operator looking at construction work/ mining for natural resources or anomalies? Next to that, the number of incidents will also make it harder to distinct between an unintentional incident or malicious act.

5 CHAPTER V – Solutions for enhancing the protection of CUI.

A range of measures can be implemented to enhance the protection of critical undersea infrastructure (CUI). This chapter examines legal solutions, operational solutions aided by technological developments, as well as common procedures and a doctrinal framework.

5.1 Legal solutions

Updating and adapting the international legal framework for the protection of underwater infrastructure will likely require both modernization of UNCLOS and the development of supplementary agreements, protocols, and cooperative mechanisms. UNCLOS was negotiated in the 1970s and early 1980s, before submarine cables, offshore energy interconnectors, and seabed infrastructure became critical to global economic and national security. The following measures are seen as essential:

5.1.1 Establish Underwater Critical Infrastructure as a Distinct Legal Category

UNCLOS currently treats submarine cables largely as an aspect of the freedom to lay and maintain cables, rather than as critical infrastructure essential to national security and economic resilience. Articles 112-115 focus primarily on cable damage and liability but do not provide a comprehensive security regime. A future protocol could formally recognize submarine telecommunications cables, electricity interconnectors, and strategic pipelines as CUI, and create enhanced protection standards like those applicable to civil aviation, maritime safety, or critical energy infrastructure.

5.1.2 Close the EEZ and Continental Shelf Jurisdictional Gap

One of the most significant weaknesses of the current framework is that many incidents occur in EEZs or on the extended continental shelf zone, where coastal state enforcement powers are limited and jurisdiction can be uncertain. Legal reform could:

- Explicitly authorize coastal states to investigate and enforce laws against intentional interference with underwater infrastructure located in their EEZ or on their continental shelf.
- Clarify arrest, detention, and evidence-collection powers.
- Create concurrent jurisdiction between coastal states and flag states in serious cases of sabotage.

5.1.3 Create a specific International Offence for Intentional Damage

Current UNCLOS provisions require states to criminalize cable damage, but implementation varies considerably. Many legal systems were designed primarily for accidental damage rather than deliberate sabotage (Hartmann and Lott, 2025) An international agreement could

define intentional damage to underwater critical infrastructure, attempted sabotage, and facilitation or financing of sabotage.

5.1.4 Strengthen Vessel Transparency Requirements

Many incidents involve vessels operating under flags of convenience, complex ownership structures, AIS manipulation, or shadow-fleet practices. These factors complicate attribution and enforcement. Possible reforms could include mandatory disclosure of beneficial ownership, stronger controls on vessel registries, and international standards for vessel tracking near critical infrastructure.

5.1.5 Establish International Investigation Mechanisms

Unlike aviation accidents, there is currently no dedicated international mechanism for investigating damage to underwater infrastructure. A new framework could establish joint international investigation teams, standardized forensic procedures, shared satellite, AIS, and maritime surveillance data, and common evidentiary standards.

5.1.6 Introduce Due-Diligence Obligations for States

A modernized framework could require states to exercise reasonable due diligence to prevent their territory, vessels, or companies from being used to damage underwater infrastructure. Such obligations could include monitoring vessels flying their flag, investigating suspicious maritime activities, and criminalizing intentional attacks within national legislation.

These measures would significantly reduce legal and jurisdictional gaps, thereby improving the security and resilience of underwater critical infrastructure.

5.2 Operational solutions

A prerequisite for the effective protection of Critical Underwater Infrastructure (CUI) is the establishment of a comprehensive overview of existing assets and their relative importance. In the absence of such visibility and prioritization, NATO and MARCOM risk dispersing scarce resources across a broad range of infrastructure without adequately addressing the most significant vulnerabilities. Therefore, conducting a systematic triage assessment that evaluates both the criticality of assets and their exposure to potential threats is essential. This approach enables a risk-based allocation of resources, ensuring that protection and defense efforts are focused on those assets whose compromise would have the greatest operational, economic, or strategic impact.

After having made the distinction about which CUI to protect and assets to use, increased patrols near critical undersea infrastructure could mitigate the risk of any attacks. Surface assets can be supported by unmanned underwater vehicles (UUVs) for the mapping and inspection of critical underwater infrastructure (CUI). These robotic systems have been developed to operate collaboratively, enabling the monitoring and protection of offshore

energy installations, subsea cables, pipelines, and other maritime infrastructure. One vehicle can be equipped with high-sensitivity cameras, sonar systems, magnetometers, and advanced artificial intelligence algorithms to detect, classify, and assess potential threats. A second vehicle can be dedicated to detailed mapping and inspection tasks, while also supporting the operation, maintenance, and integrity management of offshore and subsea infrastructure. NATO's MCM forces are equipped with enough systems and platforms for monitoring and/or surveilling CUI. These systems could also be used for post-incident forensics to determine the causes of damage, collect evidence, support attribution, and facilitate legal accountability (distinguishing between accidental and deliberate actions) of further taken steps.

Another effective approach to safeguard CUI is to enhance its resilience through the implementation of protective measures. The CUI needs to be equipped with built-in sensors (acoustic, optic and magnetic) for detecting (malicious) threats. Another option would be to surround the CUI with a network of sensors for intrusion detection. These active/passive systems can make use of automated track behavior algorithms categorizing subjects. We need to take notice of the fact that: any detection system is as good as its response to the incident. Incident response involves mitigating and/or countering the identified threat. When a quick response is needed, we can make use of 'common' air or surface assets. When any explosive device is found close to CUI, we could make use of explosive collection ROVs or divers with atmospheric suits (up to 300 meters). As for any system, testing the network of sensors to find out its weaknesses will contribute to further improvement of that system.

Finally, infrastructure owners and operators, whether state-owned or privately owned, (generally) have the right to protect infrastructure. A technical solution for this is to diversify and make sure there's enough redundancies, just by making sure there are many of them. Helped by an adequate capacity to repair (e.g. by unmanned underwater vehicles) will make a single act of sabotage less decisive in causing serious problems.

5.3 Common procedure and doctrine

At the core, the decisive driver is not policy but a shared sense of vulnerability: because undersea systems are globally interconnected, security can only be effective if it is coordinated. Therefore, we can expect high feasibility for common procedure at the regional or alliance (NATO, EU, G7) level because of a shared threat perception (notably hybrid threats from state actors), already existing interoperability structures and increasing joint exercises and operations. In these organizations we can expect standard operating procedures (SOPs) for surveillance and monitoring, incident response, information sharing, and protection of sensitive operational data. A 'federated' model for the protection of CUI can cover these elements:

1. A threat model shaped by a range of interconnected risks, including hybrid warfare, cyber-physical attacks on critical infrastructure, and covert sabotage operations.

2. Common operational principles to emphasize persistent seabed surveillance, multi-domain awareness across the maritime, air, cyber, and space domains, and the ability to ensure rapid attribution and response to emerging threats.
3. Information-sharing architecture built on trusted networks that connect navies, governments, and industry operators to enable timely coordination, intelligence exchange, and collective action.
4. A security baseline underpinned by robust cybersecurity standards, including International Organization for Standardization (ISO) and NIS2 [1] frameworks, complemented by physical protection measures and comprehensive redundancy and resilience planning.
5. A Lifecycle protection approach.

A lifecycle protection approach ensures that infrastructure is secure, resilient, and continuously protected from creation to operation and, if needed, recovery, rather than treating protection as a single, isolated step. The stages in this approach are:

1. Design

Protection begins at the planning and design phase.

- Risks and threats are identified early (e.g., sabotage, cyber risks, environmental hazards).
- Security features are built into the infrastructure itself (e.g., redundancy, hardened materials, secure communication systems).

2. Deployment

This covers installation and commissioning.

- Safe and secure installation procedures are followed.
- Measures are taken to prevent interference or tampering during construction and laying (e.g., surveillance, restricted access zones).

3. Monitoring

Once operational, the infrastructure is continuously observed.

- Use of sensors, surveillance systems, and data analysis to detect anomalies or threats.
- Regular inspections and real-time monitoring to ensure integrity and performance.

4. Recovery

Focuses on response and restoration after damage or disruption.

- Incident response plans are activated.
- Repair capabilities and contingency measures (e.g., backup systems, rapid repair teams) are implemented to restore functionality quickly.

[1] NIS2 is a directive of the European Union aimed at protecting digital infrastructure, in particular critical infrastructure.

There is evidence that common doctrine is already beginning to emerge in different organizations. NATO has taken important steps toward developing an operational framework through the establishment of the Critical Undersea Infrastructure Coordination Cell (CUICC) at NATO Headquarters and the Maritime Centre for the Security of Critical Undersea Infrastructure within MARCOM. These initiatives indicate the gradual formation of a military-operational doctrine focused on undersea infrastructure protection, encompassing threat detection, deterrence, and civil–military coordination. NATO's Baltic Sentry operation (2025), launched to deter and respond to acts of sabotage against critical maritime infrastructure, illustrates the practical application of this emerging approach.

The EU has been building a regulatory and resilience framework. One example of this is the EU Cable Security Action Plan (2025) encompassing infrastructure mapping, coordinated risk assessments and stress testing and resilience planning. This action plan is designed in a whole resilience cycle approach: prevent, detect, respond & repair and deter (European Parliament, 21.02.2025).

Another example is the development of a Cable Security Toolbox (2026) including risk mitigation measures to address risk scenarios. This toolbox initially includes recommendations on a strategic level: e.g. diversity of routes and landing locations, reduce exposure to non-EU suppliers and operators, and promote co-ordination between industry, member states, NATO and international bodies. Second, recommendations are made on a technical/support level: e.g. ensure adequate physical and cyber protection of submarine cables, increase monitoring, surveillance and detection capabilities, and strengthen maintenance and repair capabilities (European Commission, Jan 2026).

Industry already has a well-established framework that consists of e.g. ISO subsea and pipeline standards, international standards developed by the ISO that define best practices, technical requirements, and safety criteria for offshore oil & gas systems, especially subsea (underwater) equipment and pipelines.

6 Case Study

This case study consists of a structured analysis of a real-world incident involving undersea infrastructure, undertaken to identify and understand threats, evaluate the effectiveness of protection measures, and derive lessons for enhancing future resilience. The following format is used:

Context:
A description of the infrastructure's location, type, key stakeholders involved, and its strategic importance in supporting essential services, connectivity, and broader economic and societal objectives.

Threat or Incident:
Identification of whether the threat or incident is natural (e.g., earthquake or fishing activity damage), accidental (e.g., ship anchor dragging), or deliberate (e.g., sabotage, espionage, or hybrid warfare).

Response and Protection Measures:
Actions and safeguards implemented to protect and respond to threats, including surveillance systems (e.g., sonar, satellites, and patrol vessels), legal frameworks (e.g., UNCLOS and national legislation), military or coast guard operations, and industry-led mitigation measures such as cable rerouting and deployment of repair vessels.

Outcomes:
Assessment of the severity of the damage, and the resulting economic, operational, and political consequences.
Lessons Identified: Identification of vulnerabilities exposed by the incident and the resulting recommendations in monitoring, resilience, redundancy, risk management, and policy or regulatory frameworks.

EstLink 2 (Baltic Sea) Cable Disruption

Context:
The EstLink 2 is a submarine power cable linking Estonia and Finland across the Baltic Sea. It has a length of approximately 170 km (including submarine and land sections), with the purpose of integrating Baltic and Nordic electricity markets, improving energy security, and supporting price stability and cross-border trading.

Incident:
There was a sudden drop to zero power flow experienced on the 25th of December 2024 that triggered an automatic shutdown of that cable, and the immediate reliance on EstLink 1 and other regional interconnections. Preliminary investigations indicated physical damage to the cable, most likely caused by external mechanical impact. The contributing factors likely were the dragging of a ship's anchor, the limited physical protection and the potential geopolitical risk (the incident occurred during heightened geopolitical tension in the region).

Response:
Following the incident, the cable was automatically shut down to prevent further damage. Grid operators promptly activated contingency plans and rebalanced electricity flows using alternative interconnectors and local generation capacity to maintain the stability and reliability of the power system. An investigation was launched to determine the cause and extent of the incident. This included the deployment of remotely operated vehicles (ROVs) and sonar scanning equipment to inspect the subsea cable and identify any physical damage. Grid operators and relevant agencies also coordinated with maritime authorities to trace vessel activity in the area, while analysts reviewed Automatic Identification System (AIS) ship-tracking data to identify vessels that may have been operating near the cable at the time of the incident. These efforts were aimed at establishing the sequence of events and supporting any necessary repair and accountability measures. Repair operations began with the mobilization of specialized cable repair vessels equipped to conduct complex offshore interventions. Once on site, technical teams worked to precisely identify and verify the fault location using diagnostic data and subsea inspection tools. The damaged section of cable was then carefully retrieved from the seabed, brought to the surface for repair or replacement, and subsequently reinstalled. After completion of the repair work, the cable was tested and returned to service to ensure safe and reliable operation of the interconnector.

Outcomes:
The disruption had significant impact on the regional energy market, reducing cross-border transmission capacity by approximately 650 MW, increasing electricity price volatility in the Baltic states, and creating greater dependence on local generation and alternative electricity imports. From a system reliability perspective, EstLink 1 was able to absorb part of the transferred load but could not fully compensate for the lost capacity, resulting in increased strain on regional power grids and a reduced redundancy margin. Economically, the incident contributed to higher wholesale electricity prices, generated potential indirect costs for industries and consumers, and required operators to incur additional repair and inspection expenses. Strategically, the event highlighted the vulnerability of critical subsea infrastructure and prompted broader discussions at both NATO and EU levels regarding the protection and security of vital energy infrastructure.

Lessons Identified:

Key lessons learned from the incident highlight the need for stronger protection and resilience of critical infrastructure. Subsea cables require enhanced physical safeguards, particularly in high-risk areas, through measures such as deeper burial and protective shielding. Effective monitoring and detection capabilities are also essential, including real-time tracking of nearby vessel activity and the integration of Automatic Identification System (AIS) data into infrastructure risk management systems. The disruption further demonstrated that, despite the availability of dual links such as EstLink 1 and EstLink 2, a single incident can still have a significant impact on transmission capacity, emphasizing the need for additional interconnections and more diversified energy sources. Finally, the event underscored the growing connection between critical infrastructure security and geopolitical risks, highlighting the importance of coordinated protection measures and joint security frameworks at the EU and NATO levels.

Recommendations focus on strengthening the resilience, protection, and long-term sustainability of critical energy infrastructure. From a technical perspective, cable protection should be enhanced through expanded burial and armoring in high-risk areas, complemented by the deployment of seabed monitoring sensors and early-warning systems that alert operators when ships approach critical infrastructure. Operationally, countries should improve cross-border incident response coordination and conduct regular emergency exercises to prepare for potential grid disruptions. At the policy level, stricter maritime regulations should be enforced around critical infrastructure, including the designation of protected cable corridors and the introduction of stronger penalties for negligent anchor dragging. In the longer term, energy security can be improved by diversifying interconnection routes, increasing renewable energy generation within the Baltic states, and investing in grid flexibility and energy storage solutions to reduce vulnerability to future disruptions.

7 CHAPTER VI- What NATO Needs

Based on the foregoing analysis, several strategic recommendations can be formulated for NATO member states:

1. Develop a NATO-Wide Critical Undersea Infrastructure Doctrine. A common doctrine would improve interoperability and ensure a unified response to both deliberate attacks and accidental disruptions. This doctrine will align member states on shared definitions of threats and vulnerabilities, standard operating procedures for monitoring, reporting, and responding to incidents, common rules for coordination between civilian and military authorities, and harmonized resilience and security standards for cables, pipelines, and offshore energy infrastructure.

2. Strengthen Maritime Domain Awareness. Early detection is essential for preventing disruptions and enabling rapid intervention. NATO members should expand their ability to detect suspicious activity around undersea infrastructure by increasing the deployment of seabed sensors, unmanned underwater vehicles (UUVs), and autonomous monitoring systems., integrating satellite, airborne, naval, and subsea surveillance networks, establishing real-time information-sharing mechanisms among allies, and utilizing artificial intelligence to identify anomalous vessel behavior near critical assets.

3. Enhance Intelligence Sharing and Threat Assessment. A common operational picture will improve decision-making and deterrence. Nations should create a dedicated framework for CUI intelligence cooperation that includes continuous exchange of threat intelligence between military, intelligence, and law-enforcement agencies, joint assessments of state and non-state actor capabilities, shared analysis of emerging hybrid threats and sabotage techniques, and regular dissemination of threat warnings to infrastructure operators.

4. Build Credible Deterrence Against Sabotage. A stronger deterrence posture can reduce the likelihood of deliberate attacks. NATO should increase the costs of hostile actions targeting undersea infrastructure by publicly declaring that deliberate attacks on critical infrastructure may trigger collective consultation and response mechanisms, improving attribution capabilities through forensic, intelligence, and surveillance tools, conducting visible patrols in vulnerable maritime areas, and expanding joint exercises focused on infrastructure protection.

5. Deepen Public-Private Cooperation. Effective protection requires close collaboration between governments and industry. Because most undersea infrastructure is owned and operated by private entities, NATO nations should establish permanent liaison mechanisms with industry stakeholders, share relevant threat information with operators, develop joint

contingency and crisis-management plans, encourage investment in security-enhancing technologies.

6. Increase Joint Exercises and Training. Exercises strengthen readiness, coordination, and interoperability. NATO should regularly conduct multinational exercises that simulate cable and pipeline sabotage, hybrid warfare scenarios, large-scale communication outages, energy supply disruptions, complex repair and recovery operations.

7. Clarify Legal and Regulatory Frameworks. Reducing legal ambiguity will facilitate faster and more effective responses. NATO allies should promote harmonized national legislation concerning infrastructure protection, clear procedures governing intervention in exclusive economic zones and international waters, improved legal mechanisms for investigating and prosecuting sabotage, and greater alignment between NATO and EU regulatory initiatives.

8. Invest in Research and Innovation. Emerging technologies will be critical for addressing increasingly sophisticated threats. Allies should support industry with technological innovation in autonomous underwater surveillance systems, advanced seabed sensor networks, and artificial intelligence-enabled anomaly detection.

9. Institutionalize a Lifecycle Resilience Approach. This lifecycle approach ensures that resilience is built into infrastructure planning and operations from the outset. NATO nations should adopt a framework that addresses three stages of infrastructure security:

- Prevention – risk assessments, deterrence, and hardening measures.
- Detection – persistent monitoring and intelligence sharing.
- Response – coordinated military, civilian, and industrial action.

The fourth stage, Recovery – rapid repair, restoration, and lessons learned is a stage that needs to be addressed by Industry.

8 Conclusion

Critical Undersea Infrastructure has become a strategic asset whose protection is essential for maintaining global connectivity, energy security, economic stability, and national resilience. The growing range of accidental and deliberate threats, combined with legal constraints and operational challenges, underscores the need for a more coordinated and proactive approach to security.

This study demonstrates that effective protection requires not only enhanced monitoring, surveillance, and rapid-response capabilities, but also resilient infrastructure design, redundancy, and robust repair capacity. The legal measures that were introduced would significantly enhance the protection, resilience, and security of underwater critical infrastructure by improving prevention, attribution, enforcement, and international cooperation.

The increasing alignment among allies on the nature of the threat creates favorable conditions for the development of a common doctrine based on shared threat assessments, standardized procedures, information sharing, and common resilience standards. Emerging initiatives by NATO, the European Union, and industry stakeholders indicate that such a framework is already taking shape.

The EstLink 2 incident further illustrates the real-world consequences of infrastructure disruption and the importance of preparedness and cooperation. Ultimately, safeguarding critical undersea infrastructure will depend on sustained international collaboration, technological innovation, and a lifecycle approach to resilience that integrates prevention, detection, response, and recovery.

NATO member states should adopt a comprehensive and coordinated approach to protecting critical undersea infrastructure by developing a common doctrine, strengthening maritime domain awareness, enhancing intelligence sharing, and building credible deterrence against sabotage. Effective protection also requires deeper public-private cooperation, regular joint exercises, and clearer legal and regulatory frameworks to improve preparedness and response. At the same time, sustained investment in research, innovation, and advanced monitoring technologies is essential to counter increasingly sophisticated threats. Finally, NATO should institutionalize a lifecycle resilience approach that integrates prevention, detection, and response measures across all stages of infrastructure planning and operation. Together, these measures will enhance the Alliance’s ability to safeguard critical undersea assets and maintain collective security, economic stability, and operational resilience.

ANNEX ALFA - List of abbreviations.

Abbreviation	Explanation
ACT	Allied Command Transformation
AIS	Automatic Identification System
COE	Centre of Excellence
CUI	Critical Undersea Infrastructure
CUICC	Critical Undersea Infrastructure Coordination Cell
EU	European Union
ISO	International Organisation for Standardization
MARCOM	Maritime Command
NATO	North Atlantic Treaty Organisation
NMCM	Naval Mine Counter Measures
NMW	Naval Mine Warfare
NMW COE	Naval Mine Warfare Centre of Excellence
ROV	Remotely Operated Vehicle
SOP	Standard Operating Procedure
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UUV	Unmanned Underwater Vehicle

ANNEX BRAVO - Bibliography

Sean Monaghan, Otto Svendsen, Michael Darrah, and Ed Arnold NATO's Role in Protecting Critical Undersea Infrastructure December 2023
NATO Media Centre NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure May 2024
Eoin Micheál McNamara (NATO review) Reinforcing resilience: NATO's role in enhanced security for critical undersea infrastructure August 2024
MARCOM presentation Protection of CUI: the operational perspective September 2024
Mid- Atlantic Ocean Assessment Critical Undersea infrastructure 2024
P. Hopkins (Penspen) PIPELINES: Past, Present, and Future. 2007
A. Lott The law of the sea perspective September 2024
TeleGeography Submarine Cables FAQ 2024
Research and Markets Submarine Power Cable Market - Global Forecast 2026-2032 August 2026
Huacan Fang, Menglan Duan in Offshore Operation Facilities Submarine pipelines and pipeline cable engineering. 2014
Offshore technology Underwater arteries – the world's longest offshore pipelines September 2014
Daniel Runde et all (Center for Strategic and International studies)

Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition August 2024
Anna Petrig Conference on Operational Maritime Law September 2024
S. Akhmetkaliyeva (Eurasian Research Institute) General Environmental Impacts of Subsea Pipelines 2020
Giorgios Kostoudis (Risk Intelligence) Underwater critical infrastructure security, how the worlds connectivity remains vulnerable October 2023
E. Kappel (Oceanography) Undersea Natural Hazards October 2015
Anna Cooban (CNN) Suspected sabotage shuts another European gas pipeline. October 2023
Amy Paik, Jennifer Counter (Atlantic council) International law doesn't adequately protect undersea cables. January 2025
J. Hartmann, Alexander Lott The Prosecution 'Gap' for Attacks on Subsea Cables and Pipelines November 2025
Halog, Margat, Staderman Legal Considerations on the Protection of Subsea Cables in the International and National Legislative Framework
Lightbox (Transition) The 'underwater' domain: the new global race is played out in the ocean depths. July 2024
Alex Westley Do Nothing: An Alternative Opinion on Critical national Infrastructure and Seabed Warfare February 2024
Henri van Soest, Harper Fine Vital Yet Vulnerable: Undersea Infrastructure Needs Better Protection March 2024
International Institute of Humanitarian Law San Remo manual on international law applicable to armed conflicts at sea

1994
European Commission: Security and resilience of EU submarine cable structures, Jan 2026)
IMO MARPOL: International Convention for the Prevention of Pollution from Ships 1973/1978