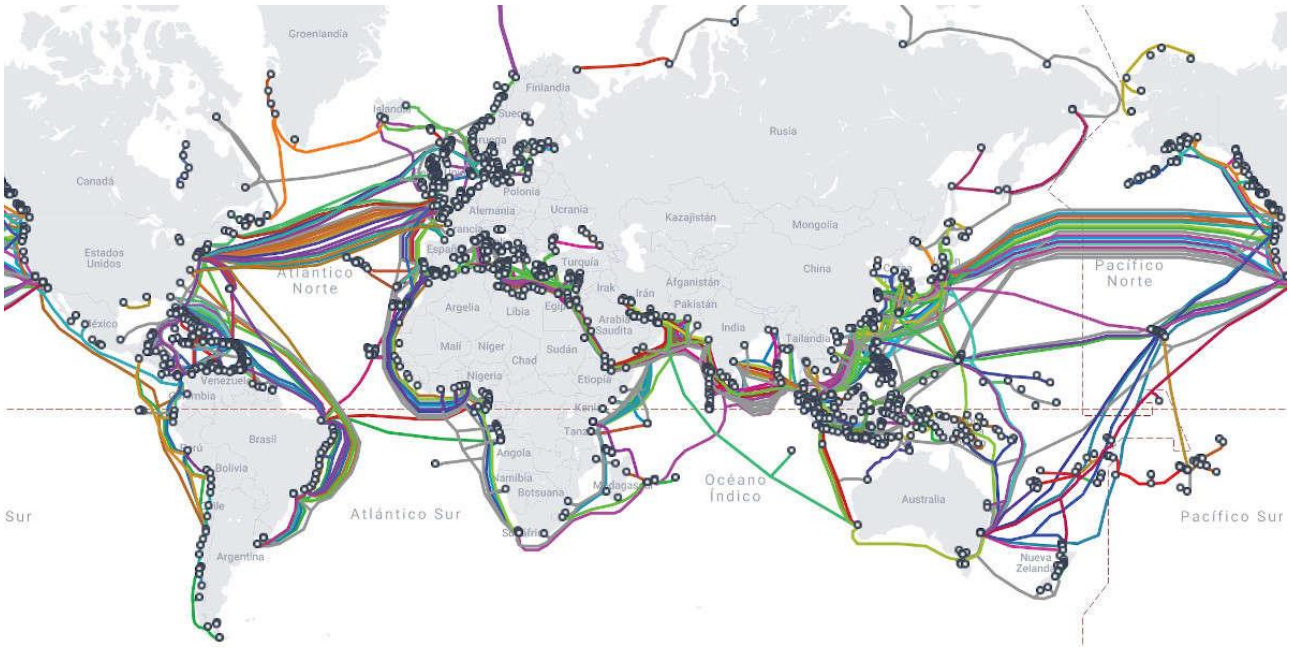
Naval Mine Warfare Centre of Excellence

Critical Undersea Infrastructure (CUI): threats, challenges, and solutions for enhancing its protection



Ostend 2025

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.

1 Contents

EXECUTIVE SUMMARY

The protection of critical undersea infrastructure (CUI) is challenging and raises questions that need to be answered. This paper is to highlight legal, technical, and operational challenges and possible solutions to these challenges.

From the legal point of view, one challenge is related to the freedom of navigation for vessels at high seas. This will make prevention of any malicious act, hard. Besides that, because 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, there is no effective regime to ensure that the responsible party is held directly accountable. Finally, CUI can be seen as a legitimate military target, so the perpetrator might see CUI as a valid target for attack according to the law of war during an armed conflict.

Looking at the technical challenges we can start by saying that we lack accurate CUI mapping, resulting in an incomplete assessment of risks and vulnerabilities. Besides that, we need to be aware that there are not a lot of technical skills required in sabotaging CUI. This will make controlling CUI a lot tougher. Finally, expertise gained within the Naval Mine Warfare (NMW) community is only beneficial in shallower waters. The NMW community is not really used to work in deeper waters, strengthened by the fact that Mine Counter Measures (MCM) systems are not designed to go that deep.

From an operational point of view, we are looking at the difficulty of prioritizing which CUI to protect, the enormous amount of mileage to cover and it's not the main task for our crews to look for acts of sabotage.

Enhancing cooperation between various initiatives is seen as one of the possible solutions for enhancing the protection of CUI. Fusing the existing intelligence picture across nations, the private and public sectors, and multinational and maritime domains is seen as a necessity. Besides that, regarding building a CUI network (community of trust), different initiatives are already in place. From a coordination perspective, within governments, decisions need to be made on who will have a seat at the table. Protection of CUI is not only a military 'issue' but should involve people from the energy and transportation sector, the police, the tech sector and the offshore industry.

One of the legal options mentioned is the creation of a global CUI protection plan. An intergovernmental organization (e.g. International Maritime Organisation (IMO)) needs to establish internationally recognized protocols under such a plan that deters actions against undersea cables and pipelines. This plan should give jurisdiction to the cable owner's state, creating a deterrent effect to any perpetrator. The European

Union (EU) Space law, covering the safety of critical space infrastructure, can (maybe) serve as an inspiration for this plan.

There are different technical solutions for the problem at hand, ranging from the use of long range/ long endurance autonomous underwater vehicles, through distributed acoustic sensing to a network of sensors for intrusion detection. In the case that a device would be found attached to a cable (or pipeline), explosive- collection remotely operated vehicles or divers with atmospheric diving suits can be used.

From an operational point of view, we first need to assess criticality versus vulnerability to a range of threats to direct the limited resources available. We want the question: 'What puts the 'C' in CUI?' answered. Seabed mapping, by hydrographic/ MCM assets or by the companies who have laid the infrastructure is critical in obtaining this information. After that, we need to look at means for constant surface and subsurface surveillance of the area.

Operational and technical challenges might be relatively easy to be dealt with. The hardest part will be to come up with universal legislation to protect CUI in such a way that the (possible) perpetrator will rather think twice before acting.

1 CHAPTER I: INTRODUCTION

1.1 General

Subsea infrastructures, such as high-speed data cables and underwater pipelines, are critical for our modern way of life. 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 and more frequently 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), highlights 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)

The main inspiration for this study came from presentations during the seminar on CUI in December 2023, held at the NATO HQ in Brussels, Belgium.

This study has been initiated by the Naval Mine Warfare Centre of Excellence (NMW COE). It will be presented to Allied Command Transformation (ACT) as part of concept development work for 2025.

1.2 Aim

The aim of this study is to give an overview of the threats, challenges, and possible solutions in relation to the protection of CUI. By writing this document, we want to inform the (NMW) Community of Interest (COI) about those aspects.

1.3 Scope

The focus of this study is on legal, technical, and operational challenges and, when possible, make the connection with Naval Mine Warfare.

1.4 Definitions

To avoid misunderstanding, we are using the following definition for CUI: 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.

1.5 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, p.1). The first permanently transatlantic 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 cable. 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)

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.

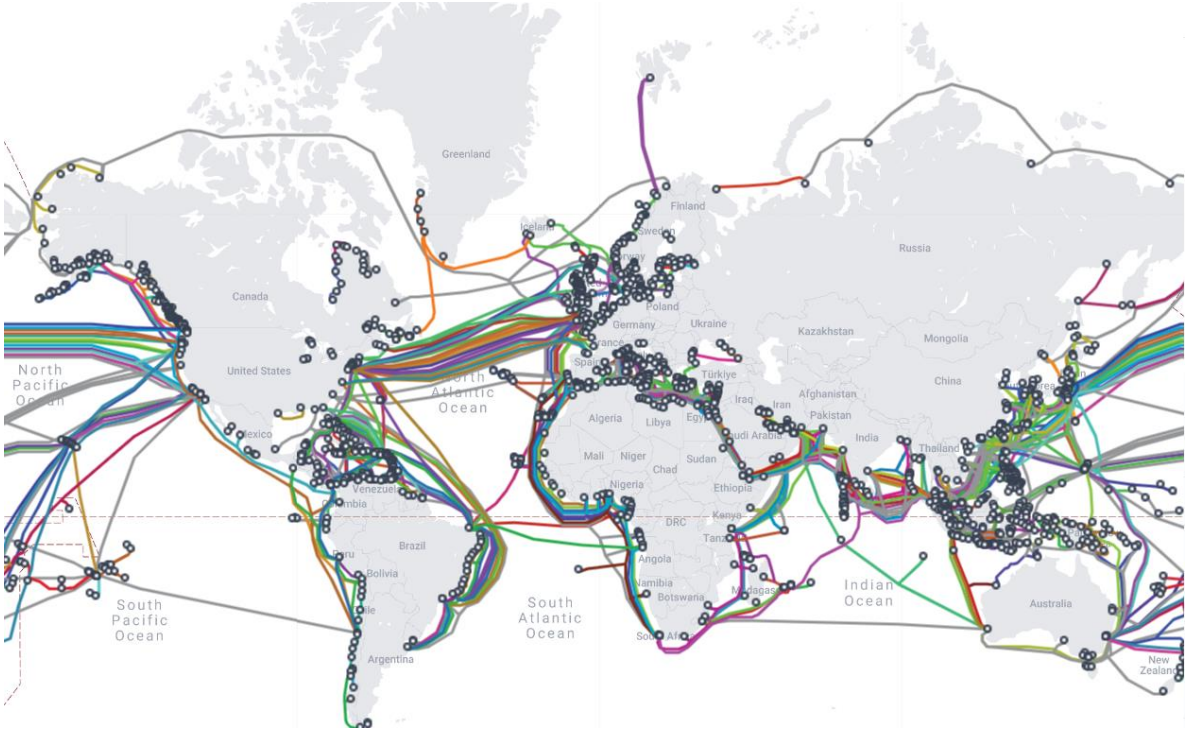


Fig. 2. Overview of the world's submarine cables 2024. Source: TeleGeography

We are looking at protecting these cables and pipelines: but against who or what? What are the threats? We need to discuss this in 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). 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).

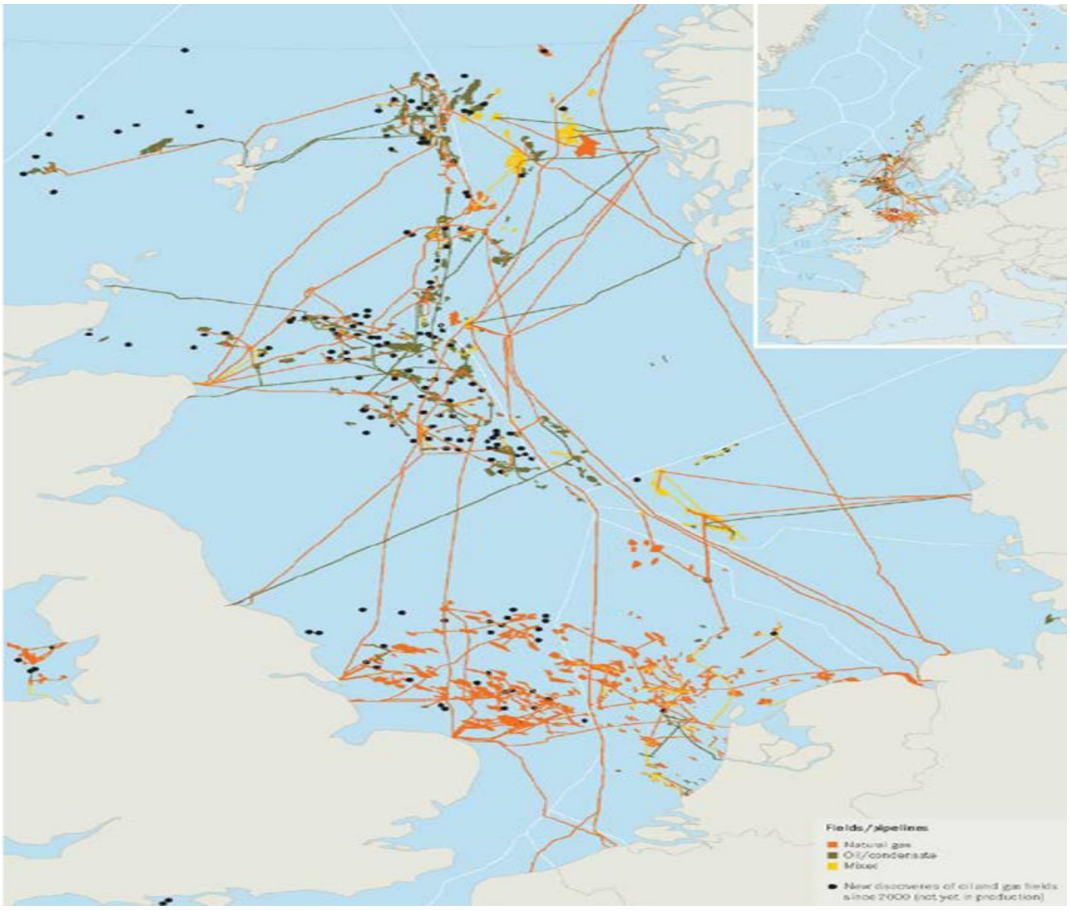


Fig 3. Map of offshore oil and gas pipelines in the North Sea (Source: Research Gate)

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).

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: Challenges regarding the protection of CUI

4.1 Legal Challenges

There are multiple legal challenges surrounding the protection of CUI. I will highlight a few of those:

Before explaining the first challenge, 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 challenge 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).
A question related to the lack of mandatory power 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). 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 caught, who will be the one(s) to react? Cables, have no flags. In a countries' TTW it seems quite clear. But what about

the (majority of) shareholders' nationality, the role for the country where the company is registered or the importing/exporting countries of the energy.

A second challenge is that critical underwater infrastructure may 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). When 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, CUI might become a military target.

A third challenge is that we are dealing with national interests, different national 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 Technical challenges

There are a variety of technical challenges when overlooking the protecting of CUI.

First, it requires limited technical expertise and resources to damage them. This enlarges the number of adversaries capable of damaging CUI.

Second, there is the absence of an accurate mapping of existing cable infrastructures and the resulting lack of a consolidated EU-wide assessment of risks, vulnerabilities, and dependencies (van Soest and Fine, 2024, L.92-95). Where exactly is this infrastructure located? What does this infrastructure look like?

Third, depth is a challenge: Greater than 1000m, faults are mostly caused by natural processes (geological or current abrasion). It is exceptionally difficult for humans to directly affect infrastructure at these depths (Westley, 2024, L.35-36). When we look at depths from a NMCM point of view, the current systems available within our allies are not equipped to work at depths even below 300 meters. Besides that, removing explosive devices or intelligence gathering devices by means of underwater robots, is not our specialty.

Fourth, there are limits to the use of underwater sensors. Sensors organized through Underwater Wireless Networks (UWN) can cover larger seafloor areas or volumes while minimizing the energy cost related to communication (Gkikopouli et all, 2012) but still face challenges in terms of energy limitation, low data rates and unreliable communication (Felemban et all, 2015). Faulty sensor data may significantly weaken the overall quality of the combined data from several sensors or any derived model.

This is particularly an issue for wireless sensor networks covering large areas, where the overall measurement performance of the network is highly dependent on the data quality from individual sensors (Skalvik et all, 2023, pg. 1). Continuous maintenance of these networks, to ensure optimal quality and effectiveness will be a challenge, especially in deeper waters.

4.3 Operational challenges

First, which vital infrastructure does one specifically want to protect? What puts the 'C' in CUI? An important question, that needs to be answered, when you want to respond quickly in the best possible way. There is no (real) prioritization made amongst different nations/industry where to aim at. 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 Baltic Sea, North Sea and large parts of the Mediterranean Sea are. When we then look at area (distance) from a NMCM perspective: our assets can only cover 24 nm2/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.

There are many ways to strengthen the protection of CUI. In this paper, I will discuss five of them.

5.1 Better cooperation between countries/entities.

A critical step in transforming maritime domain awareness (MDA) to improve detection and identification of threats to CUI will be *fusing* the existing intelligence picture across nations, the private and public sectors, and multinational and maritime domains (e.g., air, sea, subsea, space, and cyber) (Moneghan et all, 2023, 87).
A good example of this fusing is NATO's Maritime Centre for Security of Critical Undersea Infrastructure (MCSCUI) at MARCOM. It is a networking and knowledge centre dedicated to the security of undersea energy pipelines and cables that assists the Commander of NATO's Allied Maritime Command. The NMCSCUI provides situational awareness, assists in identifying vulnerabilities, and supports operational-level information exchange among the CUI-Network "community of trust" to deter, defend, and respond to threats against CUI.

Regarding the building up of a CUI network for enhancing MDA, collecting intelligence, and sharing of information/knowledge, there are some more examples of initiatives being taken. I will highlight a few:

NORDIC Co-Operation: the Nordic and Baltic ministers of digitalisation laid the foundation for strengthened cooperation on critical underwater infrastructure. A secure digital infrastructure is a prerequisite for Allied countries' competitiveness and for securing the national need for electronic communication and access to digital services.

Critical Seabed Infrastructure Protection (CSIP), a Permanent Structured Cooperation (PESCO)- project: the goal of this project is to ensure the protection of infrastructures from natural events, intentional attacks and deliberate sabotage, using Unmanned Underwater Vehicles (UUVs) (embracing both Autonomous Underwater Vehicles (AUVs) and Remotely Operated Vehicles (ROVs)) and mobile and resident hosts.

North Sea Agreement: The agreement between Belgium, Denmark, Germany, the Netherlands, Norway, and the United Kingdom is expected to focus on information-sharing across Europe, through the creation of a platform for registering and sharing data about suspicious movements at sea (van Soest and Fine, 2024, L.93-97). The joint declaration focuses on resilience and prevention.

Seabed Security Experimentation Center (SeaSEC): SeaSEC is an international partnership between the Netherlands, Denmark, Germany, Finland, Norway, and

Sweden aiming at accelerating the development and adoption of capabilities to secure undersea infrastructure in shallow waters (North Sea and Baltic)

Norway and Germany's ministers of defense signed a joint statement on a proposal to further strengthen the Alliance's role in protecting critical underwater infrastructure by creating regional CUI hubs for different maritime areas in NATO's area of responsibility "The hubs would monitor underwater infrastructure and bring in regional expertise to improve situational awareness in the underwater domain. Personnel and capabilities of respective national authorities could be used to detect suspicious activities and deter potential adversaries".

5.2 Actions that focus on coordination.

Within governments, decisions need to be made on who will have a seat at the table. Discussions should involve people in energy security, critical infrastructure, police, technology, transportation, and intelligence. Although civil and military entities are not automatically allowed to work together, there needs to be coordination between the various initiatives on subsea infrastructure protection. For example, the new EU Critical Entities Directive mandates member states to protect critical infrastructure. Meanwhile, the EU-NATO Task Force on the resilience of critical infrastructure recommended EU and NATO staffs to collaborate further on the monitoring and protection of critical maritime assets. Staff exchange has increased through the establishment of the Brussels-based NATO Critical Undersea Infrastructure Coordination Cell (CUICC) and a London-based Maritime Centre for the Security of Critical Infrastructure. RAND (Research and Development) policy think-tank and others have encouraged NATO to establish an international undersea infrastructure protection corps, combining both government and private-sector defense approaches to protect and maintain subsea assets. Governments need to make sure that these initiatives work efficiently together, without duplication (van Soest et all ,2024, L. 108-137). A good example of an interagency, interservice operation, which comprehends the use of multiple and different assets and platforms is Italy's 'Operazione Fondali Sicuri'.Information coming from every fleet component , including surface, underwater and air assets, as well as other armed forces and agencies, are fused at the Navy's Fleet Command (CINCNAV) to monitor traffics and highlight connected anomalies or specific vessels of interest operating nearby underwater infrastructures.

5.3 Legal initiatives (to be taken)

An intergovernmental organization such as the United Nations or its International Telecommunication Union (ITU) needs to establish internationally recognized protocols under a formalized protection plan that deters actions against undersea cables and prioritizes the security of digital communications. Such a protection plan should give jurisdiction to the cable owner's state. Under such a plan, the fact that the

cable owner's state could take the perpetrator's state to court might make intentional saboteurs think twice, creating a deterrent effect, especially if fines or remediation costs are significant. It should also consider non-state actors, such as armed groups or large multinational business companies, who could interfere with the cables. UNCLOS, as a traditional treaty between states, does not hold nonstate actors responsible, even in a scenario in which a terrorist group were to inflict damage (Paik and Counter, 2025, L. 73-81). It's clear that the same is applicable for the protection of undersea pipelines, albeit by other international entities (e.g. United Nations Economic Commission).

The proposed EU space law is a good example of new regulations being set. This law will set rules on space traffic management, and will provide a framework to ensure the safety of the critical space infrastructure, so why not create this kind of law on CUI? A law on CUI (protection) enhancing the level of security and resilience of CUI operations, as well as their safety and sustainability, to encourage the development of resilience measures, foster information-exchange on incidents as well as cross-border coordination and cooperation.

It's sometimes suggested that the regulations stated in the International Convention for the Prevention of Pollution from Ships (IMO, MARPOL, 1973/1978) could be of use of preventing any possible sabotage attempts. Although an inspection of the condition of the ship or its equipment would certainly prevent the ship from sailing for a while, the inspection can only take place in port or offshore terminal. Furthermore, when a ship is unduly detained or delayed, it shall be entitled to compensation for any loss or damage suffered.

5.4 Technical solutions

As stated in 'The 'underwater' domain: the new global race is played out in the ocean's depths: Protecting the underwater infrastructure requires appropriate regulations, *advanced technology,* and a targeted military strategy (Transition lightbox, 2024, p.1). The role of industry becomes critical. Commercial partners, particularly those in offshore energy, deep-sea exploration, and subsea telecommunications, possess advanced capabilities and technologies for operating at different depths. Collaborating with industry not only fills current capability gaps but also accelerates innovation and adaptation in underwater defense technologies.

I will highlight some of the technical solutions.

One way is to enhance the resilience by putting into place 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 would be found close to CUI, we could make use of explosive collection ROV [1] 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.

One other technical solution is to diversify and make sure there's enough redundancy, 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. One good example of diversification leading to a more redundant communication system is NATO's hybrid space-submarine architecture ensuring infosec of telecommunications (HEIST)- program aimed at developing a crucial backup plan for the global internet in case undersea cables are damaged or sabotaged. The project aims to quickly detect cable damage and reroute data through satellites.

Finally, a third way is to use UUVs for CUI mapping and inspection. Robots have been designed to operate in tandem, monitoring offshore energy parks, cables, pipelines, and other underwater infrastructure. One robot, equipped with sensitive cameras, sonars, magnetometers, and AI algorithms to identify threats. A second one is used to map, inspect, and help in the operation and maintenance of any infrastructure at sea.

5.5 Operational solutions

First, because there's no clear overview of which CUI to protect and a consecutive lack of prioritization, an initial triage assessment of criticality versus vulnerability to a range of threats can help MARCOM and NATO (Nations) to direct limited resources to protecting and defending those assets most at risk (Moneghan et all, 2023, 86).

Second, continuous surveillance on CUI. After having made the distinction about which CUI to protect, increased maritime patrols near critical undersea infrastructure could mitigate the risk for any attacks. With the launch of Baltic Sentry, NATO is already coming up with a way to deter any future attempts by a state or non-state actor to damage critical undersea infrastructure. NATO also established TASK FORCE X, a specialized initiative focused on delivering capabilities that exploit emerging and disruptive technologies, including autonomous systems and artificial intelligence into maritime operations to enhance the Alliance's situational awareness of sea lines of communication and safeguard critical undersea infrastructure. Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, the Netherlands, Norway, the United Kingdom, and

[1] E.g. Seaeye FALCON, or VVLAI

Sweden are members of the Joint Expeditionary Force (JEF), which has taken an active role in countering threats against subsea infrastructure protection, including the recent launch of joint maritime patrols. Beside these initiatives, NATO could consider establishing an “SNMG3” to focus on protecting CUI in northern Europe, focused on the Baltic Sea, North Sea, and Norwegian Sea (the areas of highest CUI density) (Moneghan et all, 2023, 85). Performing Route Survey on CUI- lines would be another option. Route Survey will give any nation, not only a continuous presence in the area, but also a continuous confirmation of anomalies. The role of industry is critical in this system. Private sector stakeholders—particularly those operating and maintaining undersea cables, pipelines, and energy infrastructure—possess unique technical expertise, real-time data, and advanced monitoring capabilities.

Third, establishing safety zones. UNCLOS article 60 states: The coastal State may, where necessary, establish reasonable safety zones around such artificial islands, *installations,* and structures in which it may take appropriate measures to ensure the safety both of navigation and of the artificial islands, *installations,* and structures. All ships must respect these safety zones and shall comply with generally accepted international standards regarding navigation in the vicinity of artificial islands, installations, structures and safety zones. This can at least give the coastal State some control over the critical undersea infrastructure in their Exclusive Economic Zone (EEZ)

Fourth, special attention should be made on making the protection of CUI an integral part of any (NATO) exercise and training program. Additionally, MARCOM will deliver messages highlighting CUI-related events during these NATO exercises and demonstrate and communicate NATO's ongoing effort to monitor CUI.

6 CHAPTER VI- Conclusion

We will start by saying that because it requires limited technical expertise and resources, it's merely impossible to, always and anywhere, prevent a perpetrator, from damaging critical undersea infrastructure. But we can make a solid effort in trying to prevent malicious acts.
The most important step that needs to be taken is to answer the question: What puts the 'C' in CUI? When it is clear which infrastructure has the highest priority to protect, we can come up easier with solutions for enhancing its protection.
The obvious technical solution is investing in technologies which are already available. UUVs, and intrusion detection systems can be easily obtained, and cable sensors are already used by cable companies. Besides that, as part of their redundancy-plans, companies are already using the 'safety in numbers'- methodology, meaning that if one cable breaks, another can take over its functionality. Finally, navies (the MCM community) should start purchasing underwater robots, capable of removing and relocating any device attached to CUI. An appropriate training needs to be part of this purchase.

Operationally a lot of initiatives are already undertaken. NATO recently launched Baltic Sentry, a 'vigilance activity' aimed at deterring, detecting, and countering any attempts by Russia's "shadow fleet" to sabotage critical undersea infrastructure in the Baltic Sea. NATO Task Force X, leveraging emerging and disruptive technologies, including autonomous systems and artificial intelligence, was also launched to play a role in deterring acts of vandalism against critical undersea infrastructure. The UK led, Joint Expeditionary Force, had already launched operation Nordic Warden, to help enhance security and protect Critical Undersea Infrastructure in the Baltic.
Besides these initiatives to enhance MSA and create persistent surveillance, Allied assets can be used for mapping the critical underwater infrastructure. We must not forget that we need to perform a thorough assessment of the criticality first. After all, our resources are limited.

The biggest challenge will be dealing with the legal aspects connected to the issue. Because legislation is outdated, and only provides limited options in bringing any perpetrator to court, the need for new legislation is obvious. A CUI protection plan, in which it is stated that the cable owner's state could take the perpetrator's state to court might make intentional saboteurs think twice. Maybe the proposed EU space law, which will provide a framework to ensure the safety of the critical space infrastructure, could help as a blueprint for this CUI protection plan.

ANNEX ALFA - List of abbreviations.

Abbreviation	Explanation
ACT	Allied Command Transformation
AUV	Autonomous Underwater Vehicle
COE	Centre of Excellence
COI	Community of Interest
CSIP	Critical Seabed Infrastructure Protection
CUI	Critical Undersea Infrastructure
CUICC	Critical Undersea Infrastructure Coordination Cell
EEZ	Exclusive Economic Zone
EU	European Union
HEIST	Hybrid space-submarine architecture Ensuring InfoSec of Telecommunications
ITU	International Telecommunication Union
JEF	Joint Expeditionary Force
MARCOM	Maritime Command
MCM	Mine Counter Measures
MCSCUI	Maritime Centre for Security of Critical Undersea Infrastructure
MDA	Maritime Domain Awareness
NATO	North Atlantic Treaty Organisation
NMCM	Naval Mine Counter Measures
NMW	Naval Mine Warfare
NMW COE	Naval Mine Warfare Centre of Excellence
PESCO	Permanent Structured Cooperation
ROV	Remotely Operated Vehicle
SEASEC	Seabed Security Experimentation Centre
SME	Subject Matter Expert
SNMG	Standing NATO Maritime Group
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UWN	Underwater Wireless Networks
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
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
Laurance Reza Wrathall The Vulnerability of Subsea Infrastructure to Underwater Attack: Legal Shortcomings and the Way Forward 2010
Amy Paik, Jennifer Counter (Atlantic council) International law doesn't adequately protect undersea cables. January 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
Yachi Chiang. A Legal Perspective on the Protection of Critical Infrastructure: The Case of Taiwan's Undersea Cables. September 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
CJOS COE Seabed Operations: Contextual Relevance and Environmental Considerations 2024
Skalvik, Saetre, Foysa, Bjork, Tengberg (Frontiers website) Challenges, limitations, and measurement strategies to ensure data quality in deep-sea sensors April 2023
Gkikopouli A., Nikolakopoulos G., Manesis S. A survey on underwater wireless sensor networks and applications 2012
Felemban E., Shaikh F. K., Qureshi U. M., Sheikh A. A., Qaisar S. B Underwater sensor network applications: A comprehensive survey. 2015
Christian Schaller Critical Maritime Infrastructure and the Regime of the EEZ: A Blank Cheque for Saboteurs? July 11, 2024
Innovations Origins How our vital undersea infrastructure is monitored April 2023
IMO MARPOL: International Convention for the Prevention of Pollution from Ships 1973/1978