»Dr. Karl A. Lamers Peace-Prize« Essaywettbewerb 2024

75 years of NATO - is the strongest alliance in history fit enough to defend all European member states against any security threats and deter all potential aggressors?

Threats to Critical Undersea Infrastructure as a NATO Security Concern

Is NATO fit for the new frontier below sea level?

Dipl.-Jur. Veit Niklas Vogler

vogler.veit@gmail.com

+491742133942

Nova School of Law Lisbon

Master's in Law and Security

I. Introduction

Every day, humanity consumes an immense amount of physical and digital resources. These resources create an immense traffic and an essential part of this traffic happens below sea level.

The term critical undersea infrastructure, also known as submarine or underwater infrastructure, describes the entire network of power cables, pipelines and optic data cables.[1] While the first two supply populations with daily energy needs, the latter is estimated to carry up to 99% of all intercontinental data traffic.[2] Scholars as Surabhi Ranganathan have gone so far calling them the "out-of-sight arteries of globalization".[3]

In tense geopolitical times, the age of so-called Hybrid Warfare has brought special attention to the strategic impact of this vital network – and its vulnerabilities. Hybrid Warfare encompasses all clear distinctions of peace and conflict, of civilian or military targets and of kinetic and non-kinetic warfare.[4] Every vulnerability of a competitor is an opportunity to be exploited.

In the following, this work will examine the strategic importance of submarine infrastructure for the North Atlantic Treaty Organization (NATO), analyze current threats and discuss the legal and operational framework used for its defence. Lastly, propositions for improvements will be made.

II. Strategic Importance of Critical Undersea Infrastructure for NATO

Given the data and resource traffic undersea, the importance of subsea infrastructure encompasses not only economic but therefore also geostrategic dimensions. The global economy is reliant on its functioning. Especially a serious disruption of the data cables, carrying financial transfer information with an estimated value of 10 trillion US Dollars, could destabilize economies.[5]

Additionally, even military operations increasingly rely on data cables. In 2008, breaks in undersea cables between Egypt and Italy caused a significant drop in U.S. drone flights in Iraq, plummeting from hundreds to mere tens per day.[6] The dependence on subsea cables will grow as military applications of 5G expand, including intelligence, command and control, and the use of unmanned and autonomous vehicles

[1] Cyfirma 2024.
[2] Cyfirma 2024.
[3] Ranganathan in Vatanparast 2020 p.1.
[4] NATO, Bilal 2021.
[5] Vatanparast 2020 p.1.
[6] Wall/Morcos 2021.

Even though the dependence on these cables rises and the rapidly progressing digitalization as well as the AI-revolution push for even more data transfer capabilities, the attention for the security concerns regarding these digital arteries is still quite limited.

Voices of reason have spoken up in the past without getting too much attention. In 2016, U.S. Vice Admiral James Foggo and Alarik Fritz raised concerns about a "fourth battle of the Atlantic," which encompassed dangers to underwater infrastructure such as oil rigs and telecom cables.[7] The following year, the UK's Chief of the Defence Staff disclosed previously classified information about Russian threats to undersea cables, describing them as a new hazard to modern life.[8]

The North Atlantic, the main NATO influential zone, has one of the highest cable densities in the world.[9] This demonstrates the relevance of threats, but also the resilience in this region. The more data cables there are, the less impactful are the disruptions of single cables. The Global South is generally more susceptible to interruptions due to fewer redundancies and lower cable density and the lack of land cable alternatives compared to the Global North.

Furthermore, two thirds of global gas and oil is being extracted below sea level or is at least being transported by sea.[10] Disruptions endanger energy security, a recurring policy issue since the full-scale Russian invasion of Ukraine in 2022. The significance of natural energy resources has been a hot topic in many domestic politics. Additionally, strikes against pipelines have the potential to create disastrous spillover effects for the natural environment and designated commercial fishing areas.

III. Vulnerabilities

A report by the Center for Strategic and International Studies goes as far as stating that NATO is not capable of effectively protecting the European Critical Infrastructure against increasing Russian aggression.[11]

The Russian navy possesses two primary methods to directly threaten undersea cables: submarines and surface vessels capable of deploying autonomous or manned submersibles. An example of the former is the *Losharik* spy submarine, which likely had the deep-sea capability to map or destroy cables before it was decommissioned due to a fire in 2019, and most likely the nuclear-powered *Poseidon*.[12] Among surface ships, there is the *Yantar*, which, despite being labeled a research vessel, is believed to function as a spy ship capable of deploying submersibles to attack and destroy cable segments.[13]

[7] Foggo/Fritz 2016.
[8] BBC 2017.
[9] Atlantic Centre 2022 p.4.
[10] NATO 2023.
[11] CSIS 2023.
[12] CSIS 2023.
[13] CSIS 2023.

Most notably, NATO staff has already voiced concerns of existing explosive devices on cables and pipelines in the Baltic Sea which may be ready to be detonated at any moment.[14] This corresponds to alleged reports by private infrastructure companies.

The recent instances of interference with critical underwater infrastructure reveal vulnerabilities – even though mainly non-Russian actors were in the spotlight.

In the beginning of October 2023, the Balticconnector gas pipeline between NATO members Finland and Estonia was damaged by a ship's anchor being dragged along the ocean floor. Additionally, two telecom cables were damaged alongside the pipeline.[15] Investigations pointed to another geopolitical competitor of NATO: China.

The Chinese container ship Newnew Polar Bear has turned out to be the main suspect of the Finish investigation. Although deliberate damaging of the infrastructure cannot be proved, the pattern of damage and the ship's immediate return to China have raised questions. Given similar Chinese actions leading to internet disruptions at the coast of Taiwan, a strategic intention is likely.[16]

The debate of the security of underwater infrastructure among NATO countries reached its high on 26th of September 2022, when two Nord Stream pipelines near the Danish island of Bornholm, intended for Russian gas transport to Germany, were severely damaged through an underwater detonation.[17] Until today, the attack could not be attributed to any actor. Given the difficulties in such an operation, a state involvement is likely. Even though suspicious Russian ship maneuvers had been reported at the site before the attack, later intelligence pointed towards a pro-Ukrainian group. The incident ended the debate on the continuation of Russian gas supply to Germany, which had already begun to restructure its energy imports - a major challenge for the new European Russia policy. No matter the perpetrator, the attack highlighted the vulnerability of NATO's energy supply network undersea.

Even though not affecting NATO infrastructure, the damaging of multiple data cables in the red sea through the sinking of a cargo ship in February 2024 has highlighted the threat for submarine cables posed by non-state actors.[18]

The locations of cables and pipelines are usually remote, far from constant supervision and publicly known – making their defence extremely difficult. Confidential cable locations would make planned attacks harder, but also significantly increases the risk of accidental damage through civilian ships.

Apart from the dangers of damage or destruction of the cables, wiretapping of strategic communication cables is another concern. Already in the 1970's the United States intelligence

[14] Eichhorn 2023.
[15] Politico 2023.
[16] Atlantic Council 2024.
[17] Gozzi 2024.
[18] DW 2024.

services managed to install a device to spy on Russian undersea communication cables in the Western Pacific.[19] This adds to the always present danger of cyberspace attacks targeting cable operating companies and therefore endangering the functioning and the integrity of the whole undersea network.

IV. The Current Frameworks for Resilience

1. The Legal Framework Issue

The legal regime governing undersea infrastructure and especially the questions of resilience and defence is still underdeveloped. A recent report by the *Atlantic Council* concluded that International Law is not fit to protect undersea cables.[20]

Underwater infrastructure is mainly not situated on national soil but found in either coastal waters or even in international waters, including the high sea. Therefore, jurisdiction, responsibilities and legal resilience are not clear cut.

(1) The Law of the Sea

The UN Convention on the Law of the Sea of 1982 is the primary legal regime applicable, but does not provide extensive coverage.

Undersea infrastructure and infrastructure parts in coastal waters are usually included in a state's territorial waters of 12 nautical miles, according to Articles 2 to 4 of the Convention. The coastal state is able to exercise its sovereignty, its jurisdiction and, under certain conditions, may defend infrastructure from attacks and threats that are not perceived as the allowed "innocent passage" of ships in those waters.[21]

Much more complex are cables situated out of the territorial waters of a state. Behind these, the Exclusive Economic Zone (EEZ) of Article 55 and the Continental Shelf of Art. 79 of the Convention find application.[22] In this perimeter, all states are permitted to the laying of submarine cables and pipelines as well as affiliated repairs and maintenance. The coastal state does exercise some exclusive rights and freedoms, but the sovereignty over the cables is none of them.

The legal rules governing the High Sea according to Article 86 of the Convention lack even any exclusive rights of cable or pipeline owners – instead the Articles 113 to 115 grant the responsibility of persecuting any damage to infrastructure to the flag state of the ship causing the damage. This is highly ineffective given the current threat landscape through state

[19] Wendorf 2022.
[20] Atlantic Council 2024.
[21] UNCLOS Art. 17.
[22] UNCLOS Art. 57.

sponsored naval vessels. Unmanned submarines or subsea drones are also not accounted for in this regulation.

But even when not confronted with High Sea cases, the jurisdiction to persecute damages of infrastructure is doubtful. For example, the Nord Stream pipeline traverses various jurisdictions, starting in Russian internal waters and passing through the Russian territorial sea, exclusive economic zone, and continental shelf. It then crosses the exclusive economic zones and territorial waters of Finland, Sweden, Denmark, and Germany, ultimately ending in German internal waters.[23]

Consequently, multiple laws could apply. This legal diversity poses challenges and does not even offer an answer regarding the legality of an active defence.

(2) Defence under International Law

As long as not in territorial waters, no legal state sovereignty is applicable to the cables – and therefore no coercive defense measures are permitted by International Law.

The Use of Force as inherent right of Self-Defence derives from Article 51 of the United Nations Charter – but is only applicable in the case of an "armed attack".

As the International Court of Justice has made clear, only "the most grave forms of the use of force" meet this threshold.[24] Limited operations that do not have the necessary "scale and effects" or the "circumstances and motivations" are not sufficient enough to trigger the right to self-defence.

It is highly doubtful that an isolated incident like the covert damaging of undersea cables or pipelines in international waters would constitute such an armed attack. Without a sovereign state as victim of the attack, a legal argument would lack strength. The mere ownership of the cable by a state or a company that is situated in a state does not convince – state practice for such a claim is missing in Customary International Law.[25]

Given the current legal regime, regulation of subsea infrastructure is neither transparent nor effective. Looking at the new threat landscape it also lacks any permission for effective resilience.

2. NATO Operational Framework for Resilience

[23] Mudric 2010.
[24] Azaria/Ulfstein 2022.
[25] Azaria/Ulfstein 2022.

Already in its 2011 Allied Maritime Strategy, NATO expanded its focus to critical energy and data subsea infrastructure.[26] Since then, especially accelerated through the Russian invasion, the Alliance's resilience has come a long way.

At the July 2023 Vilnius NATO summit, an agreement for the establishment for the Maritime Centre for the Security of Critical Underwater Infrastructure at NATO's Allied Maritime Command (MARCOM) was finalized.[27] It provides closer coordination for the Allies to better identify and mitigate existing vulnerabilities through deterrence and defence.

Additionally, since the beginning of 2023, NATO maintains the Critical Undersea Infrastructure Coordination Cell in its Brussels Headquarters, which build on the cooperation of civilian and military stakeholders and encourages cable companies to step up their security measures.[28] Deepening collective efforts, NATO also established the EU NATO Task Force on Resilience of Critical Infrastructure 2023.[29] It produces valuable insights on current vulnerabilities of the energy and data networks of the Alliance and its European partners.

Through these institutions, NATO conducts risk assessments and builds capabilities for worst-case attack scenarios that could render large parts of the network inoperable. Most importantly, it closely monitors Russian warfare tactics directed against critical infrastructure in the Ukraine conflict to develop learnings and best practices.

The volume of sea and air patrols in the Baltic Sea has also been increased by the Alliance.[30] But pipeline and cable networks are massive. Worldwide, there are 485 undersea cables with a total length of over 900 000 kilometers.[31] Even only surveying directly NATO affiliated structures around the clock comes close to a mission impossible.

V. Recommendations

1. Putting additional pressure on cable companies

National governments must ensure that companies uphold the highest security standards. Therefore not only the dialogue with private cable companies must go on but additional incentive is necessary. Allies should motivate operators to follow voluntary guidelines, such as those from the International Cable Protection Committee (ICPC), which sets standard procedures for cable owners and some governments. Non-member allied governments should consider joining the ICPC to strengthen the role of this non-governmental organization. If voluntary guidelines do not sufficiently encourage investment in cybersecurity, allies may need to establish mandatory requirements, similar to the U.S. response to the Colonial

[26] CSIS 2023.
[27] CSIS 2023.
[28] NATO 2023.
[29] EU 2023.
[30] NATO 2023.
[31] Chataut 2024.

Pipeline ransomware attack, which mandated cybersecurity measures for oil and gas pipelines.[32]

2. Establishment of an operational task force

While the establishment of the NATO and NATO/EU coordination centers is a vital step towards more infrastructure resilience, this is not enough yet. Military operational capacity has to increase drastically. The Alliance must maintain a continuous military presence to supervise vital infrastructure and build its deterrence capabilities.

While right now this is largely conducted by the allies independently in a soft-coordination approach, collaboration must be intensified. This may be achieved through the establishment of a Maritime Rapid Response Force (MRF). This force can be operationally similar to the Rapid Response Force that was founded after the 2002 Prague summit as a quick deployment unit.[33] Similar to the regular Rapid Response Force currently stationed in the Baltic States and other European partners, these forces could be strategically placed near potentially vulnerable maritime infrastructure for immediate deployment capabilities.

Incorporating sea, air and Special Forces units, it could provide regular patrol services and effectively coordinated deterrence through a joint Rapid Response Command. Integration of civilian cable maintenance and repair vessels would ensure immediate response capabilities in case of cable faults. As there is only an overstretched and insufficiently organized global cable ships fleet in private hands so far, state sponsored centralized action is necessary.[34]

National acquisitions of specialized vessels like recently in the Royal Navy or underwater surveillance drones will be needed and defence spending budget incentives can be used to motivate allied states to contribute.[35] Simultaneously, contingency plans for large scale cable or pipeline outages need to be further developed, maybe even through acquisition of secret reserve cables with undisclosed locations to at least guarantee the functioning of critical data flows.

3. Pushing for a new legal framework

Furthermore, to bolster legitimacy for the operational framework and create legal certainty, the legal framework governing the resilience of subsea infrastructure has to be developed further.

The UNCLOS is not fit to determine jurisdiction in case of cables damages and lacks any permissions or exclusive rights to defend the infrastructure in more distant marine zones from sabotage. Reworking the Convention and granting sovereignty rights to cable affiliated states

[32] CSIS 2024.
[33] NATO 2023.
[34] CSIS 2024.
[35] CSIS 2024.

may be one solution – but not necessarily the most promising one. The United States have neither signed nor ratified the Convention and therefore a major UN and NATO player is missing.

While some scholars argue that the Convention has entered status of Customary International Law, this cannot surely be said for every aspect of the treaty – but surely not for coming modifications.[36] Therefore a new legal regime would be more fitting. A convention on subsea cables has already existed in the past for underwater telegraph cables. [37]

Efforts to create a new treaty may be lengthy and challenging in the current geopolitical climate, but uniting competing world powers under one legal regime is a worthy goal. Drawing from 20th-century arms control experiences, major powers might share a common interest in preventing attacks on critical supply networks. As China, Russia, and the US seek stronger ties with the Global South, which is more vulnerable to disruptions due to less cable and pipeline density, a united effort could enhance their legitimacy in leading global geopolitics.

These efforts could be facilitated through the UN system in cooperation with the International Cable Protection Committee. The treaty's main goal should be granting state sovereignty over subsea cables, allowing attacked states to respond with proportionate military force per Article 51 of the UN Charter, such as warning shots, detainment, or non-lethal sinking of attacking vessels.

The International Court of Justice, supported by the International Tribunal for the Law of the Sea, shall have jurisdiction to ensure legal certainty. Only with a solid legal basis will operational defense be truly legitimate.

VI. Conclusion

The security of critical underwater infrastructure has gained significant attention in recent years, particularly due to events in Ukraine since February 2022 and subsequent Baltic Sea incidents. While NATO aims to strengthen its resilience against these hybrid threats, much work remains, especially in developing the legal framework and corresponding literature. Legal and operational measures are still needed from NATO and its European partners.

With technological advancements, the energy crisis, and rising data demands, the threat landscape is likely to expand. If Russia reallocates naval resources away from Ukraine, the capacity for attacks on underwater infrastructure will grow. Similarly, China's relationship with the West, influenced by developments in Taiwan, could also heighten risks to submarine infrastructure if geopolitical tensions worsen.

[36] Curtis 2023.
[37] DZLR 2023.

(2990 words)

Bibliography

Azaria, Danae; Ulfstein, Geir (2022): *Are sabotage of submarine pipelines an 'armed attack' triggering a right to self-defence?* https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/

Atlantic Centre (2022): *Protecting subsea data cables in Europe and the Atlantic – Challenges of a new era* https://www.defesa.gov.pt/pt/pdefesa/ac/pub/acpubs/Documents/Atlantic-Centre_PB_13.pdf

Atlantic Council (2024): *International law doesn't adequately protect undersea cables. That must change* https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/

BBC News (2017): *Russia a 'risk' to undersea cables, defence chief warns* https://www.bbc.com/news/uk-42362500

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

Center for Strategic and International Studies (2023): *NATO's Role in Protecting Critical Undersea Infrastructure* https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure

Chautaut, Robin (2024): *Undersea cables are the unseen backbone of the global internet* https://theconversation.com/undersea-cables-are-the-unseen-backbone-of-the-global-internet-226300#:~:text=About%20485%20undersea%20cables%20totaling,and%20isolated%20areas%20within%20oceans

Curtis International Law Office (2023): *UNCLOS* https://www.curtis.com/glossary/public-international-law/unclos#:~:text=Who%20has%20ratified%20UNCLOS%3F,the%20United%20States%20of%20America.

Cyfirma (2024): *Threats to Undersea Infrastructure* https://www.cyfirma.com/blogs/threat-to-undersea-infrastructure/#:~:text=Underwater%20infrastructure%3A%20Explained,99%25%2C%20including%20banking%20transactions

Deutsches Zentrum für Luft- und Raumfahrt (2023): *Legal Considerations on the Protection of Subsea Cables in the International and National Legislative Framework* https://elib.dlr.de/197998/1/Legal%20Considerations%20on%20the%20Protection%20of%20Submarine%20Cables%20in%20the%20International%20and%20National%20Legislative%20Framework.pdf

DW (2024): *Houthi attacks in Red Sea threaten internet infrastructure* https://www.dw.com/en/houthi-attacks-in-red-sea-threaten-internet-infrastructure/a-68470988

Eichhorn, Moritz (2023): *Verdacht der Nato: Russland vermint Pipelines und Kabel in der Ostsee* https://www.berliner-zeitung.de/politik-gesellschaft/verdacht-der-nato-russland-vermint-pipelines-und-kabel-in-der-ostsee-li.345567

European Union (2023): *EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure* https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

Foggo, James; Fritz, Alarik (2016): *The Fourth Battle of the Atlantic* https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic

Gozzi, Laura (2024): Nord Stream: Denmark closes investigation into pipeline blast https://www.bbc.com/news/world-europe-68401870

Mudric, Miso (2010): *RIGHTS OF STATES REGARDING UNDERWATER CABLES AND PIPELINES* https://www.researchgate.net/publication/265194864_RIGHTS_OF_STATES_REGARDING_UNDERWATER_CABLES_AND_PIPELINES

NATO (2023): *NATO Response Force* https://www.nato.int/cps/en/natohq/topics_49755.htm

NATO (2023): *NATO's maritime activities* https://www.nato.int/cps/en/natohq/topics_70759.htm#undersea

NATO (2023): *NATO stands up undersea infrastructure coordination cell* https://www.nato.int/cps/en/natohq/news_211919.htm

Politico (2023): *'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says* https://www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/

United Nations Convention on the Law of the Sea (1982)

Vatanparast, Roxana (2020): The Infrastructures of the Global Data Economy: Undersea Cables and International Law *Havard International Law Journal Frontiers* https://deliverypdf.ssrn.com/delivery.php?ID=629021065069066007028105066117016072004042024048051009122067095096091112110026118092123124006123042032124103107115120019110070119033078019018121018014027102089096004070050017097127096064113003083000080097113027092011112086097124094113073104064119009024&EXT=pdf&INDEX=TRUE

Wall, Colin; Morcos, Pierre (2021): *Invisible and Vital: Undersea Cables and Transatlantic Security* https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Wendorf, Marcia (2022): *Operation Ivy Bells: The U.S. Top-Secret Program That Wiretapped a Soviet Undersea Cable* https://interestingengineering.com/innovation/operation-ivy-bells-the-us-top-secret-program-that-wiretapped-a-soviet-undersea-cable

All sources last accessed 26.06.2024