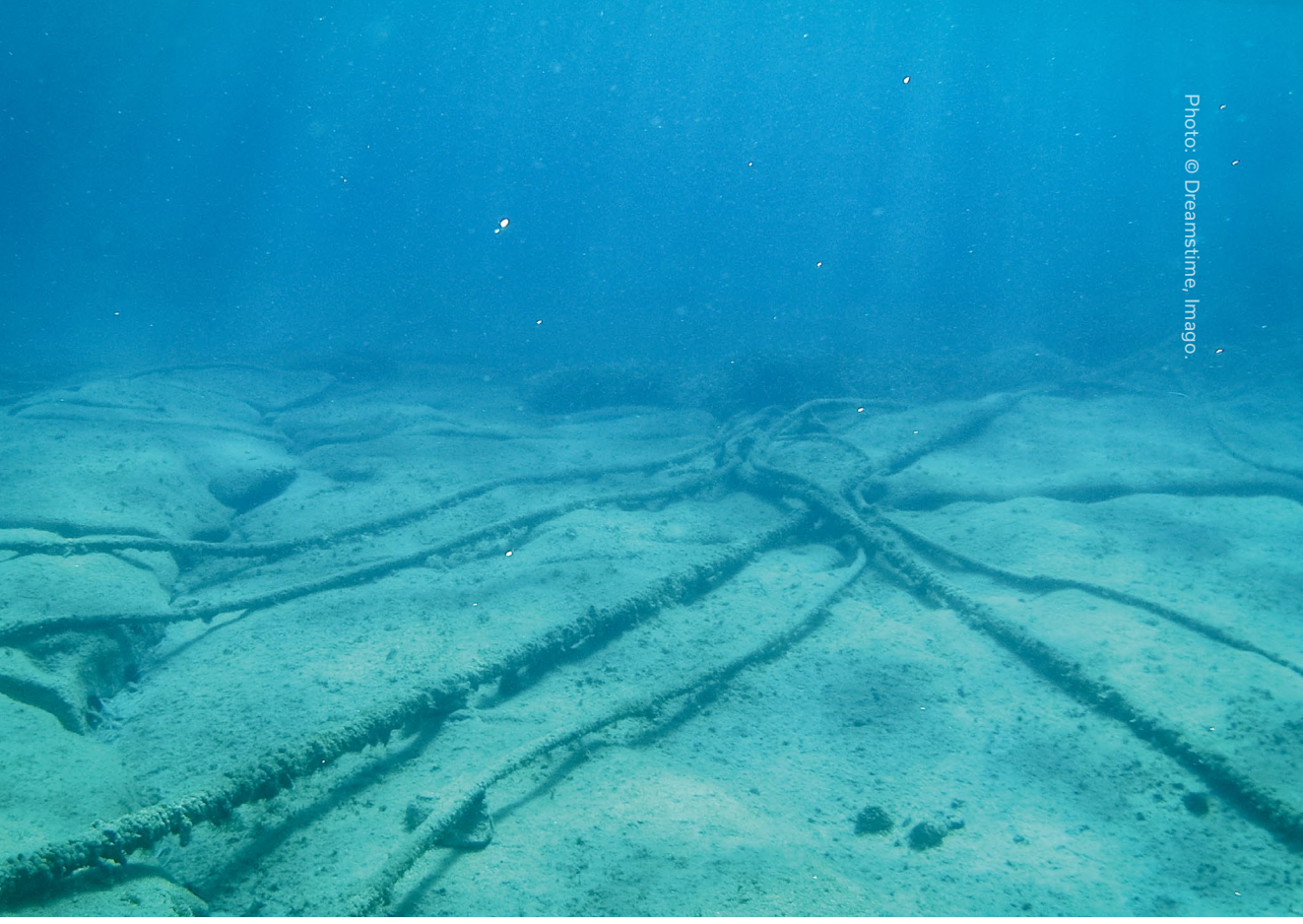

Photo: © Dreamstime, Imago.

Water

Lifelines under Threat

How We Can Make Europe's Maritime Critical Infrastructure More Resilient

Ferdinand Gehringer / Matthias Hespe

Vulnerable and lacking sufficient protection, maritime critical infrastructure is the target of hybrid warfare. The latest incidents involving submarine cables have revealed weak points that highlight an urgent need for action. However, protecting this vital infrastructure alone will not be sufficient to prevent significant disruptions in the future.

There has been an increase in incidents involving maritime critical infrastructure in the recent past, including two damaged submarine data cables in November 2024, disruptions to one submarine power cable and four submarine data cables around Christmas of the same year in the Baltic Sea region, and damage to a submarine data cable off the coast of Taiwan at the beginning of 2025. Ever since the attack on the Nord Stream pipelines in the Baltic Sea in September 2022, the security of maritime critical infrastructure has become the focus of public attention, thereby raising questions about security measures and how to deal with outages. Although there have been a number of initiatives and some progress has been made, these steps forward have been far from sufficient given the importance of this infrastructure, its vulnerability, and the actors intent on damaging it. Submarine cables, in particular, are the perfect target for hybrid warfare.

Vital Facilities – Above and below the Waterline

There is no universal definition of maritime critical infrastructure; instead, the maritime component is integrated into what is generally defined as critical infrastructure, or "KRITIS", as it is known in Germany. According to the German Federal Office for Information Security (BSI), the term denotes "organisations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences".[1]

Such organisations and facilities may have maritime relevance in sectors such as energy, information technology and telecommunications, and transport and traffic. This includes infrastructure in and on the water, such as energy supply facilities including drilling platforms and wind farms, as well as underwater infrastructure, such as pipelines, submarine data cables and submarine power cables. At the same time, critical infrastructure on land can also be categorised as maritime if it has direct maritime relevance, including basic physical and digital infrastructure belonging to port facilities and port operators as well as shipping companies, cranes and logistics centres, landing points for submarine cables and transhipment points, such as oil and LNG terminals.

Distinctive Characteristics of Maritime Infrastructure

Maritime critical infrastructure exhibits a number of distinctive characteristics that pose a particular threat to its security. Its remote location requires the use of special skills and technical equipment. Underwater infrastructure in particular – such as data and power cables or pipelines – can, depending on the depth, only be accessed using the appropriate devices and equipment. Data cables that run through the Atlantic lie at depths of up to 6,000 metres and are often several thousand kilometres long.

The ownership structures are also often complex, with several companies frequently investing jointly in submarine data cables. Planning, building and laying these cables is highly costly. For instance, the SEA-ME-WE 6 cable (South East Asia-Middle East-West Europe 6) is a 21,700-kilometre-long submarine cable

system that lies between Singapore and Marseille and cost around 480 million euros to construct. While the submarine cable infrastructure was operated for decades by consortia of state-owned telecommunications providers, rising costs, the expansion of the global data industry and increasing demand on the part of tech companies have led big tech firms such as Alphabet, Apple, Meta, Microsoft and Huawei to invest in submarine cable infrastructure, thereby taking the place of state investors and telecommunications providers.

Maritime critical infrastructure is exposed to a wide range of potential threats.

In addition, infrastructure often extends across national borders, which gives rise to complex questions of jurisdiction and grey areas from the point of view of international law. For example, the United Nations Convention on the Law of the Sea (UNCLOS) establishes clearly defined zones of national responsibility and authority,[2] but maritime critical infrastructure – especially underwater infrastructure of a transnational nature, such as pipelines and submarine cables – often passes through several such zones, each of which may be subject to a different legal framework. In its coastal waters, which are defined as the territory up to twelve nautical miles from the baseline of the land border,[3] a state has territorial sovereignty, meaning that it is entitled to take comprehensive measures to protect its maritime critical infrastructure. However, in the immediately adjacent exclusive economic zone (EEZ, up to 200 nautical miles from the baseline), this is only the case to a limited extent. Coastal states have exclusive economic rights in their EEZ and are authorised to build, operate and protect their own infrastructure in this zone. That is why, in addition to underwater infrastructure that passes through the EEZ, a significant proportion of offshore energy supply facilities – such as drilling platforms and wind farms – are also located in these areas. However, the problem is that UNCLOS does not grant a coastal state any authority to exercise sovereignty over ships travelling in its EEZ or in the adjacent high seas area; rather, this authority lies exclusively with a ship's own flag state. Consequently, the coastal state may not take any coercive measures against a foreign ship in its EEZ without the consent of the flag state, even if the ship is suspected of committing sabotage against the coastal state's critical infrastructure. There is some dispute as to whether other international conventions might provide a legal basis for measures taken by the coastal state against foreign ships in such cases.[4]

Infrastructure as a Target of Hybrid Warfare

Maritime critical infrastructure is exposed to a wide range of potential threats, including environmental impacts such as storms, landslides and seaquakes as well as accidents caused by technical or human error, such as those that result from shipwrecks or fishing activities. The majority of disruptions to maritime critical infrastructure are caused by natural or unintentional factors of this kind. Approximately 70 per cent of the damage to submarine cables is inflicted by ship anchors, dredging work or trawling.[5] In the spring of 2024, several submarine cables were damaged following an attack on the freighter Rubymar by Houthi rebels in the Red Sea. Of the 16 submarine cables that run through the Bab al-Mandab strait from the Arabian Sea to the Red Sea, three were no longer functional afterwards; they had been damaged by the anchor of the sunken freighter dragging along the seabed.[6]

In addition to unintentional incidents, deliberate harm to maritime critical infrastructure is also becoming a growing concern. Hybrid warfare is becoming more aggressive, especially on the part of Russia, but the Chinese are also pursuing more confrontational activities in Europe, and incidents involving deliberate acts of harm are on the rise. In addition to the examples mentioned above, other cases have occurred in the Baltic Sea and the North Atlantic in recent years.[7]

Sabotage and espionage of critical infrastructure are key tactics used in hybrid warfare. By carrying out attacks on critical infrastructure in order to inflict damage and potentially even cause service outages, the aim is to impair state interests by inducing insecurity and instability within society. In such cases, it is considerably more difficult for governments to respond rapidly, appropriately and in a legally compliant manner. The damage to infrastructure typically falls short of full-scale war and is generally carried out secretly, with the perpetrators' identity remaining concealed.[8] As such, it is difficult to attribute the damage to a specific actor, and it is thus by no means easy to come up with an appropriate response.

The Russian "shadow fleet" is being deployed for hybrid warfare.

Energy and telecommunications infrastructure, in particular, has become a target, with two scenarios having become more likely in the Baltic Sea region:

1. cumulative acts of sabotage carried out in quick succession on critical infrastructure aimed at causing noticeable disruptions so as to burden or entirely overwhelm state structures and have an unsettling impact on society;

2. acts of sabotage against energy infrastructure – particularly offshore wind farms – aimed at slowing Europe's progress towards the energy transition, deterring investors and prolonging dependence on fossil fuels (including Russian energy sources).

Russia operates a fleet of "research vessels" through its Main Directorate of Deep-Sea Research (also known as GUGI), which is an organisational unit of the Russian Ministry of Defence.[9] This fleet comprises more than 50 ships, including civilian research vessels, specialised Russian navy vessels and submarines that are additionally capable of carrying out reconnaissance and sabotage on facilities as well as of conducting warfare on the seabed.[10] The fleet systematically collects data on critical energy and telecommunications infrastructure in the North Sea and Baltic Sea and maps the seabed.

However, this is not the only tool used by Russia to conduct its hybrid warfare: the Russian "shadow fleet"[11] is also being deployed with increasing frequency. Last December, the oil tanker Eagle S – the vessel whose crew is suspected of having sabotaged a submarine cable between Estonia and Finland – was revealed to belong to this fleet. The Russian shadow fleet consists of tankers and cargo ships that are frequently very old and poorly maintained: they tend to operate under alternating foreign flags of smaller states, they often switch off the automatic identification system (AIS) used for exchanging ship data and routes, and they are significantly underinsured.[12] Generally speaking, nothing is known about the ownership structures. The tankers export Russian crude oil, so the fleet is effectively used to circumvent economic sanctions.[13] At the same time, the tankers also pose a significant risk to the environment and to marine conservation.

China has also stepped up its hybrid activities, as exemplified by the damage inflicted on the natural gas pipeline Balticconnector in the Baltic Sea between Finland and Estonia in October 2023. Investigations revealed that the Chinese container ship Newnew Polar Bear – which flies the Hong Kong flag – dragged its six-tonne anchor over a distance of 180 kilometres across the bottom of the Baltic Sea, thereby destroying the pipeline and two submarine data cables running nearby. Chinese authorities deny that this act was intentional, describing the incident as an accident.[14] Submarine cables off the coast of Taiwan were likewise damaged with China's involvement.[15]

Cases of sabotage and espionage are not limited to critical undersea infrastructure: other maritime critical infrastructure has been affected as

well. Incidents include flights by suspected Russian surveillance drones over harbour facilities – such as LNG terminals in Germany[16] – and over oil rigs and offshore wind farms off the coast of Norway.[17] German and European port operators and authorities have been increasingly confronted with cyber attacks, especially since the start of the Russian war of aggression against Ukraine in 2022.[18] Incidents of Russian electronic warfare have also become more frequent since then, especially in the Baltic Sea region. Satellite navigation signals are jammed, and the positions of civilian and military ships are spoofed.[19] Some shadow fleet vessels are also used for espionage purposes. These ships often call at European ports at random and are turned away from the harbours due to their condition or their cargo, but in the process they record the processes and structures of the harbours as well as the security precautions on site.

Private data cable operators are increasingly becoming a pawn in geo-economic power games between the US and China.

Even if the immediate impact of these incidents has thus far been limited and any damage is usually repaired quickly, there is clearly an urgent need to pay greater attention to maritime critical infrastructure.

Weak Points in the Infrastructure

What is required to deal with this situation is a better understanding of the existing weak points, which frequently extend beyond the infrastructure itself. The example of submarine cables clearly shows how complex the problem is.

1. *Weak Point: A Lack of Redundancies*

By transporting more than 95 per cent of international data traffic, submarine data cables serve as the backbone of global data transmission and communication, and there is currently no alternative.[20] Data transmission via satellite is (still) too slow, in addition to being more costly and more susceptible to interference.[21] Satellite transmission is thus only used in regions in which it is not possible to lay terrestrial cable.

Driven by the digital transformation, increasing numbers of new internet users and data-intensive technologies such as AI, cloud services, streaming platforms and social media, the demand for data transmission is growing rapidly.

2. *Weak Point: High Level of Dependence on Big Tech Companies*

Most submarine data cables are now financed and operated by large technology companies, which control a significant share of the global

Part of the Russian "shadow fleet"? The oil tanker Eagle S, sailing under the flag of the Cook Islands, was seized by Finnish authorities in late 2024. Its crew is suspected of having damaged a submarine cable in the Baltic Sea. Photo: © Heikki Saukkomaa, Lehtikuva, Imago.

data infrastructure, resulting in a concentration of dependency. At the same time, those companies are increasingly becoming a pawn in geo-economic power games that are being played out between the US and China. The US leverages economic pressure in order to counter Chinese competition in the construction and deployment of submarine cables that would enhance global communication. China likewise draws on state subsidies for cable construction. This was especially evident in the SEA-ME-WE 6 submarine cable project.[22]

The European Union and Germany lack infrastructure of their own that they could fall back on in the event of escalating geopolitical tensions, data blockades or other prioritisation of data transmission on the part of companies. The only exception is the EllaLink data cable, a joint project involving the EU and Brazil.[23]

3. *Weak Point: Limited Global Capacity for Damage Repair*

The limited repair capacity can result in prolonged outages.[24] Repairing submarine cables is complex and can be very time-consuming depending on their location and depth. Only a limited number of specialised ships and experts have the ability to carry out this kind of work. Currently, 77 cable-laying vessels are in operation worldwide, but only 22 of them specialise in

repairs. In addition, these ships are 28 years old on average, so in many cases, they are approaching the end of their useful life.[25] Additonally, it makes more economic sense for the operators of cable ships to use their capacity to lay new cables rather than to make repairs.[26]

4. *Weak Point: Responsibilities Are Not Allocated According to Capabilities*

Currently, responsibilities for the protection of critical infrastructure in Germany are not allocated based on capabilities. In principle, the operators (usually in the private sector) are responsible for protecting the infrastructure. It is they who must take appropriate technical and organisational measures to protect the facilities from disruption and to manage security risks. However, these operators lack ships with the appropriate capabilities to counter interference from foreign governments.

A lot of valuable time is lost due to the need for coordination when an incident occurs.

In order to ensure more extensive protection and defence against threats to underwater infrastructure, the police in Germany's individual states have executive powers in coastal waters, whereas in the exclusive economic zone, those powers lie with the federal police. The Federal Ministry of

A comprehensive overview: The Commander Task Force Baltic (CTF Baltic) was set up in Rostock to create underwater and surface situation reports for NATO. Photo: © Bernhard Herrmann, Imago.

Transport is responsible for shipping lanes and harbours but has no means of protecting them, so this protection is taken care of by the federal police. However, the relevant police authorities have only limited capabilities, especially when it comes to operating under water. By contrast, the navy does possess the relevant capabilities in principle but is only authorised to provide support via administrative assistance procedures. This situation, in which the responsible agencies lack the required skills and resources, means that a great deal of valuable time is lost due to the need for coordination and application procedures when an incident does occur.

A Set of Measures to Reduce the Number of Weak Points

Only by applying a set of measures is it possible to increase protection, minimise the risk of outages, and reduce the consequences of disruptions.

1. *Ensuring Better Protection for Strategic Hubs*

Full-scale protection of submarine cables is not possible because the cables are too long and the areas that would have to be protected are too expansive. However, there are strategic hubs around the world where cable connections are clustered and run on land, such as in Marseille, Singapore and on the west coast of Ireland. Many cable connections in the Red Sea are also close together, thereby increasing the risk of multiple instances of damage occurring simultaneously. These critical points require special protective measures on the part of operators and states so as to both deter potential attackers and enable a faster response in the event of damage. In order to ensure the security of the infrastructure, it is essential to ensure continuous monitoring by patrols both on the surface of the ocean and under water using modern, unmanned technologies, such as the German underwater drone Seekatze (Sea Cat), which can reconnoitre the seabed by means of precise sonar at depths of up to 300 metres, or Robosalp, an underwater robot currently under development that is to be able to reconnoitre regions of the ocean that are particularly remote and deep. In January, NATO deployed a fleet of ten ships to protect submarine cables and prevent sabotage in the Baltic Sea region until April, but under the Copenhagen Convention of 1857 and UNCLOS, NATO does not have the authority to block the passage of ships in international waters.

2. *Adapting the Properties and Laying Depth of the Cables*

Submarine cables have to be more robust. Currently, they are up to 15 centimetres thick, are encased in a steel cable, and are surrounded by a tar-soaked nylon mixture. This sheathing can be further reinforced, and the cables can be laid deeper in the seabed. Before installation, cable-laying ships check the seabed for potential risks, such as seabed composition and currents. Where there are major risks on the seabed itself, the cables are laid up to 1.5 metres deep in the ocean floor. This is particularly effective when it comes to avoiding the scenario of damage being caused to the cables by dragging anchors.

All players know full well that comprehensive situational awareness is also required under water.

3. *Increasing Redundancies*

It is also vital to increase redundancies. In addition to alternative and additional data transmission via other cable lines and the construction of further data cable connections, it should also be possible to use satellite systems to transmit data in the event of disruptions. The NATO project HEIST (Hybrid Space-Submarine Architecture Ensuring Infosec of Telecommunications) provides a good starting point:[27] in the event of a major attack on the cable infrastructure, data transmission is to be redirected to satellites. In addition, state resilience plans should prioritise particularly important data so that essential

data connections are instantly rerouted and maintained in the event of a large-scale outage.

4. *Expanding Repair Capacities*

The number of specialised ships has to be significantly increased so as to be able to both distribute repair capabilities regionally and initiate repairs swiftly. One possibility would be for the EU to build up its own capacity. For instance, the EU could maintain three to five repair ships that are to be made available to private operators in the event of damage while at the same time helping to ensure a more balanced sharing of the burden between the state and private companies when it comes to the upkeep and security of the infrastructure. The brunt of the burden is currently borne by private operators. Alternatively, the International Telecommunication Union (ITU) could take the lead in globally distributing repair resources, especially through the International Advisory Body for Submarine Cable Resilience, which the ITU established in partnership with the International Cable Protection Committee (ICPC).

5. *Developing Comprehensive Situational Awareness*

All players know full well that comprehensive situational awareness is also required under water. This means that the data from ships, reconnaissance aircraft, drones, satellites and submarine cable operators must be combined in a single overview. Technology such as sensors, multibeam sonar, infrared cameras and laser light sources can also be used to generate an even better image of the situation under water, which is essential when it comes to ensuring protection and rapid incident response. In any case, permit conditions should mandate that operators add more sensors and cameras when installing infrastructure. The European regulations to be implemented for the protection of critical infrastructure – that is, the NIS-2 Directive and the CER Directive – do not go far enough in this regard. Part of the remit of the Commander Task Force Baltic (CTF Baltic) established in Rostock is to provide both underwater and surface situational awareness for NATO in the future.

The navy must be equipped with enhanced underwater capabilities and be authorised to intervene more quickly.

6. *Using an AI-supported AIS Database*

The AIS of ships must be put to more effective use in order to protect submarine cables. Recorded in a database, AIS data can provide early indications of ships that have been suspect in the past, and the database can flag these ships in order to facilitate closer monitoring. This process would enable Russian shadow fleet ships to be detected more easily and to be tracked in real time. Simultaneously, these ships' inadequate insurance could provide an additional avenue for authorities to intervene.

The data could be analysed using AI-supported systems, thereby creating a risk forecast for the ships. The basis for this forecast could be the AI-operated maritime surveillance tool planned by the Joint Expeditionary Force (JEF).[28]

7. *Allocating Responsibilities According to Capabilities*

Furthermore, responsibilities need to be allocated according to capabilities. The navy must be equipped with enhanced underwater capabilities and be authorised to intervene more quickly. A framework similar to that used by the German Central Command for Maritime Emergencies could be a solution as it would enable more rapid intervention on the part of the navy in such cases. In complex crisis situations, the Central Command is assigned operational management, taking over leadership of the emergency forces and resources, specifying operational objectives and issuing orders to this effect to the relevant authorities. In terms of

maritime critical infrastructure, a similar model would be conceivable for the federal and state police forces as well as for the navy.

8. Ensuring Clear Communication and Consistent Action

In addition, swift countermeasures are needed in the event of incidents, and so too is precise, effective communication on the part of authorities and operators. Suspicious activity – be it confirmed or disproven – should be regularly shared with the public, and any investigative findings based on images and videos should be showcased for clarity. For instance, Finnish authorities acted swiftly and effectively in response to the suspected sabotage by the oil tanker Eagle S in December 2024.[29]

9. Adapting International Law

UNCLOS should include a ban on sabotage and espionage against submarine cables and pipelines (e.g. as a new Article 112a, UNCLOS), and coastal states should be invested with the relevant authority.[30] In its own EEZ, for example, a coastal state should be allowed to carry out coercive measures and investigations against foreign ships without the consent of the flag state if such ships are suspected of committing sabotage or espionage against the coastal state's maritime critical infrastructure. At present, this area remains poorly regulated – unlike the clearly defined powers over ships suspected of piracy (Art. 105, UNCLOS) or illegal fishing activities (Art. 62 (4) and Art. 73, UNCLOS).[31]

10. Boosting Infrastructure Investment

Above all, the EU must invest more in infrastructure, not least in order to reduce the current significant dependence on big tech companies that dominate investments in the expansion of cable infrastructure. Investments should focus not only on additional cable routes or repair capacity, but also on satellite systems as a redundant transmission option. The EU should either invest in infrastructure itself or support investments by European companies. The key factor here is to reduce dependence on non-European countries and companies.

Conclusion

In recent months, some coastal states have responded more quickly to the incidents in the Baltic Sea region than in previous years. Nevertheless, the security precautions for submarine cables and the measures taken to deal with outages are still inadequate. In light of the increasing risk of further incidents, there is an urgent need to take more comprehensive measures and to make life more difficult for potential attackers in the future. Only a set of smaller and larger measures can address our weak points so as to counter hybrid attacks and secure maritime critical infrastructure.

– translated from German –

Ferdinand Gehringer is a Policy Advisor on Homeland and Cyber Security in the Analysis and Consulting Department of the Konrad-Adenauer-Stiftung.

Matthias Hespe is a Policy Advisor on Maritime Security in the Analysis and Consulting Department of the Konrad-Adenauer-Stiftung.

1 German Federal Office for Information Security 2024: What are Critical Infrastructures?, in: https://ogy.de/rg35 [23 Feb 2025].
2 UN 1982: United Nations Convention on the Law of the Sea (UNCLOS), A/CONF.62/122, in: https://ogy.de/n96b [12 Feb 2025].
3 For the individual provisions regarding the definition of the baseline, see Articles 5, 7 and 14 UNCLOS, ibid.
4 Schaller, Christian 2024: Völkerrechtliche Grundlagen des Schutzes maritimer kritischer Infrastruktur, in: Voelsen, Daniel (ed.): Maritime kritische Infrastrukturen, Strategische Bedeutung und geeignete Schutzmaßnahmen, Stiftung Wissenschaft und Politik, SWP-Studie 2024/S 03, 6 Feb 2024, pp.19 ff., in: https://ogy.de/soqd [12 Feb 2025].
5 Wissen.de 2022: Unterseekabel – Schlagadern der Weltkommunikation, 24 Oct 2022, in: https://ogy.de/4bpg [12 Feb 2025].
6 Welt 2024: Nach Huthi-Beschuss gesunkener Frachter hat wohl Unterseekabel durchtrennt, 8 Mar 2024, in: https://ogy.de/b1cr [12 Feb 2025].
7 One such case was the destruction of submarine cables between the Faroe and the Shetland Islands in October 2022, see Humpert, Malte 2022: Fiber-optic Submarine Cable near Faroe and Shetland Islands Damaged; Mediterranean Cables also Cut, High North News, 24 Oct 2022, in: https://ogy.de/yb8m [12 Feb 2025].
8 Bueger, Christian / Liebetrau, Tobias 2023: Critical maritime infrastructure protection: What's the trouble?, in: Villasante, Sebastián et al. (eds.): Marine Policy, Sep 2023, pp. 4 f., in: https://ogy.de/8gtm [12 Feb 2025].
9 Gehringer, Ferdinand 2022: Undersea cables as critical infrastructure and geopolitical power tool. Why undersea cables must be better protected, Facts and Findings 495, Konrad-Adenauer-Stiftung, 22 Dec 2022, in: https://ogy.de/qg0i [23 Feb 2025].
10 Corera, Gordon 2023: Ukraine war: The Russian ships accused of North Sea sabotage, BBC, 19 Apr 2023, in: https://ogy.de/n4zd [12 Feb 2025].
11 The term "shadow fleet" refers to ships that are used for concealment tactics to smuggle sanctioned goods and circumvent economic embargoes.
12 These ships operate without the type of Western insurance that is standard in the shipping trade. They do not belong to protection and indemnity (P&I) clubs. Merchant ships are covered by hull and machinery insurance as well as by cargo insurance. There is also P&I insurance, which covers serious risks, such as oil spills and attacks. P&I insurance is provided by the International Group of P&I Clubs, which comprises a total of twelve clubs. Insured shipowners pay into their club, which pays out insurance claims on an annual basis.
13 Braw, Elisabeth 2024: The threats posed by the global shadow fleet – and how to stop it, Report Atlantic Council, 6 Dec 2024, in: https://ogy.de/2h57 [12 Feb 2025].
14 Chiappa, Claudia / Ngendakumana, Pierre Emmanuel 2023: 'Everything indicates' Chinese ship damaged Baltic pipeline on purpose, Finland says, Politico, 1 Dec 2023, in: https://ogy.de/1mdc [12 Feb 2024].
15 Wu, Huizhong / Lai, Johnson 2023: Taiwan suspects Chinese ships cut islands' internet cables, Associated Press (AP), 18 Apr 2023, in: https://ogy.de/8kzv [12 Feb 2025].
16 NDR 2024: Spionage? Drohnen über Brunsbüttel beschäftigen Politik und Polizei, 26 Aug 2024, in: https://ogy.de/y1hk [12 Feb 2025].
17 Lewis, Mark 2022: Unidentified drones over Norway's offshore platforms fuel fears of Russian threat, PBS News, 23 Oct 2022, in: https://ogy.de/ot4u [12 Feb 2025].
18 Tagesschau 2024: Kritische Infrastruktur: Mehr Cyberangriffe auf deutsche Seehäfen, 5 Sep 2024, in: https://ogy.de/bsfs [12 Feb 2025].
19 Bischoff, Kristian 2024: Maritime Dangers of GPS/AIS Spoofing and Jamming in the Baltic Sea, RiskIntelligence, 15 Jul 2024, in: https://ogy.de/ohft [12 Feb 2025].
20 Burnett, Douglas R. / Beckman, Robert C. / Davenport, Tara M. (eds.) 2013: Submarine Cables. The Handbook of Law and Policy, Leiden, p. 9; Gehringer 2022, n. 9.
21 Researchers at the Massachusetts Institute of Technology have calculated that one pair of fibres in a submarine cable can transmit more signals than 4,000 satellites in the Starlink system.
22 Gehringer, Ferdinand 2023: Geoökonomische Machtspiele unter Wasser, Standpunkt China Table, 5 Sep 2023, in: https://ogy.de/g1rz [12 Feb 2025].
23 Gehringer, Ferdinand 2024: EllaLink – how a submarine cable does more than just connect, in: Hedrich, Maximilian 2024: As relações Brasil-Europa diante do mundo em transformação, Konrad-Adenauer-Stiftung, p.101, 6 Feb 2024, in: https://ogy.de/s9ks [12 Feb 2025].
24 Submarine Telecoms Forum 2024: Industry Report 13. Reporting Trends and Repair Time, p. 88, in: https://ogy.de/zl2t [12 Feb 2025].
25 Dzieza, Josh 2024: The Cloud under the sea, The Verge, 16 Apr 2024, in: https://ogy.de/4mco [12 Feb 2025].
26 For example, the US government pays the company Subcom ten million dollars per year to be able to use two repair ships in an emergency.
27 Sawall, Achim 2024: Nato will bei Seekabel-Angriffen auf Satelliten umlenken, Golem, 9 Jul 2024, in: https://glm.io/186875 [12 Feb 2025].
28 JEF is a military partnership led by the United Kingdom that includes the Nordic states, the Baltic states and the Netherlands.

29 Special forces of the Finnish border guard boarded the tanker shortly after the incident and published photos of the operation. The ship's detention in Finland and the follow-up investigations were also backed up with clear and open communication with the public on the part of the authorities. See for example AP 2024: Finland detains Russia-linked vessel over damaged undersea power cable in Baltic Sea, NPR, 27 Dec 2024, in: https://ogy.de/uzmi [12 Feb 2025].

30 Even though UNCLOS designates acts of sabotage of underwater infrastructure on the high seas as "criminal offences", it places jurisdiction over them in the hands of the flag state of the ship that caused them and not in the hands of the state responsible for the infrastructure. UN 1982, n. 2, Art. 113, p. 64.

31 UN 1982, n. 2.