SISEKAITSEAKADEEMIA
Estonian Academy of Security Sciences
INTERNAL SECURITY INSTITUTE

EMILIA MUUGA, RAMON LOIK, GEORG-HENRI KAUP,
RAUL SAVIMAA, ERKKI KOORT

SECURITY THREATS TO THE UNDERSEA CONNECTIONS RELATED CRITICAL INFRASTRUCTURE OF THE BALTIC STATES

The Baltic Sea in the Focus of Hybrid Warfare

EMILIA MUUGA, RAMON LOIK, GEORG-HENRI KAUP,
RAUL SAVIMAA, ERKKI KOORT

Security Threats to the Undersea Connections Related Critical Infrastructure of the Baltic States

The Baltic Sea in the Focus of Hybrid Warfare

The authors thank Arnold Sinisalu, Priit Saar, and Priit Heinsoo for reviewing the manuscript and providing valuable feedback.

Second, revised, and updated edition

Cover: pixabay.com

Design and layout: Jan Garshnek

Copy-editing: Refiner Translations

Printing: Trükikoda Paar

ISBN 978-9985-67-513-7 (print)

ISBN 978-9985-67-514-4 (pdf)

DOI: https://doi.org/10.15158/nv7t-kg46

www.sisekaitse.ee/kirjastus

CONTENTS

SUMMARY

- The number of deliberate, human-induced incidents targeting subsea infrastructure in the Baltic Sea has increased precipitously since 2022. Acts of sabotage and disruption against critical undersea infrastructure remain likely in the coming years.
- Estonia and the other Baltic states are dependent on electricity, gas, and data connections running along the Baltic seabed. As a result, the risk of disruptions to critical services is greater for the Baltic states than for countries on the western shore of the Baltic Sea. This is particularly true due to the vulnerability of the NordBalt electricity connection between Lithuania and Sweden and the Estlink 1 and 2 connections between Estonia and Finland, which link the Baltic states to the European electricity market.
- Targeting critical infrastructure, including subsea infrastructure, is a key element of both China's and Russia's strategic activities, often used to pressure various states and organizations. While the primary threats to Europe's submarine cables stem from Russia, recent incidents indicate increasing cooperation in this field between Russia and the People's Republic of China.
- Numerous cases confirm Russia's active interest in and operational capability to monitor, disrupt, and, if necessary, damage the critical underwater infrastructure of European states. Meanwhile, China's activities are primarily focused on cable production, installation, and investment to secure control over global data flows. However, China's cooperation with Russia in physically damaging connections has also intensified.
- The greatest challenge in protecting subsea connections is their location in international waters, where it is unclear who holds the authority and responsibility for oversight and regulation.
- The duty to ensure the security and integrity of subsea infrastructure should not end with a country's exclusive economic zone, as this creates greater opportunities for deliberate acts of sabotage. Applicable legislation should provide effective protection for subsea connections, ensuring that perpetrators of deliberate attacks cannot act with impunity. Intentionally damaging subsea infrastructure should be deemed universally illegal, prevented, and met with an appropriate response when it occurs.
- Completely securing both land-based and subsea connections at all times is both costly and complex. Therefore, it is crucial to thoroughly assess potential risks at both regional and national levels and have detailed contingency plans in place.

- The attacks on Estlink 2 and Balticconnector highlighted a major vulnerability: restoring subsea connections may take more than six months. Particular attention must be paid to scenarios in which multiple cables are severed simultaneously, thus posing a severe threat to the continuity of critical services.
- Estonia and the other Baltic states must develop undersea infrastructure protection capabilities through international cooperation, as developing such capabilities independently would be prohibitively costly for any of the countries alone.
- The effective protection of the subsea infrastructure of Estonia and the other Baltic states requires coordination between various government agencies, closer collaboration between the state and the private sector, and building stronger partnerships with allies. Consequently, Estonia, together with its Baltic Sea allies, should adopt an active stance within NATO and EU formats on the development of undersea infrastructure protection capabilities.

INTRODUCTION

Intercontinental and cross-border data exchange, as well as electricity and gas transmission, are essential for the functioning of modern society. These systems are essential not only for the maintenance of critical services but also for the overall functioning of the economy. The infrastructure required for data transmission or gas networks cannot function without electricity. Many power plants rely on gas for electricity generation, while electricity transmission depends on internet connectivity and data exchange. Together, electricity, gas, and data networks form an integrated system in which a fault in one component can ruin the entire chain.

On average, each European country is connected to at least two other states via land-based or subsea pipelines or cables (Bueger et al., 2022, p. 25). In addition to linking individual countries, cables also connect continents. Submarine fiber-optic cables, described as the "invisible arteries" of global communication (Hendriks & Halem, 2024, p. 7), facilitate access to financial markets and enable artificial intelligence, remote work, digital public services, and the Internet of Things, among other things. Given the rapid growth in data volumes, subsea connections are becoming increasingly important, as no better alternative for data transmission currently exists (Insikt Group, 2023, p. 20). It is therefore unsurprising that, in an era of escalating geopolitical tensions, such critical connections have become significant targets for unfriendly actors (Hendriks & Halem, 2024, p. 7).

The deliberate, coordinated, and targeted sabotage of intercontinental submarine cables could have severe consequences, particularly on the continuity of critical services (French Ministry of Armed Forces, 2022, p. 23). The extensive length and poor accessibility of submarine cables make them effective targets for hybrid warfare, thus increasing the likelihood that critical maritime infrastructure will become a preferred target for hostile attacks in the future (Hendriks & Halem, 2024, p. 15). NATO's Assistant Secretary-General for Intelligence and Security, David Cattler, has repeatedly emphasized how adversarial states seek to gain a strategic advantage by threatening the security of Western internet, energy, and financial systems (Siebold, 2023; Cooper, 2023). The European Parliament (2024) has also emphasized repeated warnings from intelligence agencies about the vulnerability of the EU's critical infrastructure, as well as the threats of espionage and sabotage, warning that disruptions to critical infrastructure could have significant negative consequences for the security of the European Union.

Submarine cables serve as the invisible arteries of global communication, enabling access to critical services such as energy and telecommunications.

Hybrid warfare enables rival nuclear powers to weaken each other's capabilities and demonstrate their offensive capacity in ways that remain below the threshold of war and open conflict (Galeotti, 2019; Kofman et al., 2021, p. 68; Hendriks & Halem, 2024, p. 14). Around the world, the sabotage of submarine cables has been linked to hybrid operations,

state-sponsored terrorism, and organized crime, although the capability to officially verify such incidents is yet to be developed (Bueger et al., 2022, p. 13). International waters and the infrastructure built within them exist in a legal gray area, making them vulnerable to attack in hybrid warfare strategies. The fact that these connections extend beyond territorial waters does not make them legitimate targets, and any attempt to damage them should be treated as unlawful, as such actions directly impact the functioning of the affected states and the well-being of their populations.

Authoritarian states such as China and Russia use attacks on critical infrastructure as a means for disrupting and dividing countries and organizations in pursuit of their strategic interests.

The activities of authoritarian states, particularly China and Russia, in targeting critical infrastructure are primarily aimed at exerting pressure on various countries and organizations. The Baltic Sea region, including the Baltic states, is perceived less as a direct military target and more as a pressure point for weakening NATO, the United States, and the European Union (Galeotti, 2019; Gallagher, 2022; Kofman et al., 2021, p. 68; U.S. Army Asymmetric Warfare Group, 2015; Radin, 2017). The main threats to Europe's submarine cables originate from Russia (Frascà & Galantini, 2023, p. 59), which has accumulated considerable experience in undersea sabotage over the years and is increasingly willing to use its naval capabilities to disrupt communication networks aggressively (Wasiuta, 2023, p. 367).

Risks to critical infrastructure can materialize in two main forms: as sudden incidents with immediate consequences or as long-term pressures, such as prolonged natural processes, wear and tear, and other gradual effects (Mehvar et al., 2021, p. 1386). Threat and risk mitigation efforts can focus on two key areas: reducing the likelihood of an incident occurring and minimizing the severity of its consequences. This applies equally to submarine pipelines and cables. On the one hand, infrastructure and connection cables should be reinforced to withstand anticipated threats, particularly natural ones. On the other hand, clients and consumers who rely on critical infrastructure and submarine cables should also reduce their dependence on these systems and find ways to minimize the impact of potential risks on their own operations.

With hybrid attacks, an incident may initially appear to be the result of wear and tear, a technical fault, or an accidental mishap rather than a deliberate act. This makes planning for response and prevention more challenging. Such a situation shifts the focus toward mitigating the severity of consequences, which is often more costly than proactive risk minimization. However, assessing the effectiveness of specific approaches remains difficult (Andžans, 2021, p. 193). The sabotage of the Nord Stream gas pipeline in September 2022 clearly demonstrated how subsea infrastructure represents a critical intersection of security and economic risk for Europe, yet both national and international jurisdiction over such incidents remains inadequate.

The application of existing legal frameworks may also present challenges, as these are unprecedented and complex events. Although Swedish investigators confirmed that traces of explosives were found at the site, leading to the conclusion that an act of sabotage had taken place (Kreek, 2024), coastal states lacked sufficient jurisdiction to conduct a further investigation. The EU's High Representative for Foreign Affairs and Security Policy, Josep Borrell, also emphasized that this was a deliberate attack and underlined the need for stronger protection of the EU's critical infrastructure (European Parliament, 2022). The core issue, however, lies in establishing the legal framework for the protection of submarine network connections, as current regulations have not kept pace with evolving security challenges. Gaps and contradictions exist between legislation pertaining to territorial, economic, and international waters, as well as between the legal frameworks

of coastal states and international maritime law. Resolving these issues is particularly complex, as subsea infrastructure spans multiple domains, including maritime safety, cybersecurity, digital networks, infrastructure management, telecommunications, fisheries, shipping, and marine environmental protection.

According to the United Nations Convention on the Law of the Sea (UNCLOS), states have the right (but not the obligation) to establish regulations for protecting submarine infrastructure within their territorial waters. However, coastal states are not required to provide protection for submarine infrastructure beyond their territorial waters (UNCLOS Art. 21; Bueger et al., 2022, p. 14). Consequently, if a subsea connection cable is severed in international waters, it cannot be classified as an attack against a specific state or organization, thus leaving no legal basis for holding the perpetrator accountable. Under UNCLOS Article 113, states are only required to adopt laws and regulations ensuring that vessels flying their flag are penalized for damaging or destroying submarine infrastructure. This highlights the inadequacy of the current international legal framework in safeguarding critical infrastructure. The resulting challenge is how best to strengthen the existing international legal framework and implement it effectively at the national level (Frascà & Galantini, 2023, p. 58). We are in a situation where subsea infrastructure, faced with both physical and cyber threats, can be viewed as part of either a defensive or offensive strategy, while technological advancements in both domains are evolving at a faster pace than the legal frameworks governing the seabed.

A distinct challenge lies in the planning, construction, operation, and management of submarine infrastructure, which is predominantly owned by the private sector (Bueger et al., 2022, pp. 13–14). Russia and China, for one, actively fund various submarine cable development projects worldwide to enhance their oversight and control over data flows and leverage them for strategic advantage (Wasiuta, 2023, p. 373). The European Parliament has already expressed its serious concern, urging EU member states and the European Commission to remain vigilant regarding financial investments made by non-EU states in critical service providers within the EU and to consider the potential consequences such investments may have on the ability to prevent major disruptions. Economic dependence on non-EU states for the construction and maintenance of critical infrastructure could significantly harm the geopolitical interests of member states. (European Parliament, 2024)

We are in a situation where subsea infrastructure, faced with both physical and cyber threats, can be viewed as part of either a defensive or offensive strategy, while technological advancements in both domains are evolving at a faster pace than the legal frameworks governing the seabed.

Despite the significance and vulnerability of subsea connections, the issue of their security has received relatively little attention in Estonia. While several international studies have been conducted in recent years, they have primarily focused on intercontinental data cables and emphasized the need for further in-depth research and analysis. For Estonia, however, data transmission cannot be considered separately from other infrastructure related to the country's energy security. Therefore, in this report, alongside data connections, attention is also given to the electricity and gas infrastructure connecting Estonia to its neighboring countries.

Considering the above, it is essential to address potential security threats to Estonia's energy and data connections with neighboring states and to raise broader awareness of the risks associated with their disruption. It is important to ensure that stakeholders involved in the planning, construction, management, and maintenance of critical infrastructure are aware of these vulnerabilities to better prepare for potential threats.

This study is based on the analysis of information gathered from publicly available policy documents, strategies, development plans, incident reports, research papers, academic and popular science articles, news reports, and blog posts. Additionally, interviews were conducted with representatives of the owners and operators of Estonia's subsea infrastructure, the Deputy Director for National Security and Defense Coordination at the Government Office of Estonia, and the head of the Estonian Navy's Maritime Operations Center. Conclusions have been drawn based on publicly available information, a selection of case studies, and findings from interviews.

It is essential to address potential security threats to Estonia's energy and data connections with neighboring states and to recognize the risks associated with their possible disruption.

This research report does not aim to provide a detailed and exhaustive overview of the connections and systems necessary for ensuring critical services. Rather, it focuses on the growing vulnerabilities of subsea energy and data connections that have become increasingly prominent in recent years and suggests measures needed to mitigate these risks. This report is an updated version of a study published by the same authors in early August 2024; this version incorporates the latest developments and events from the past year, references the latest sources, and presents additional conclusions and recommendations accordingly.

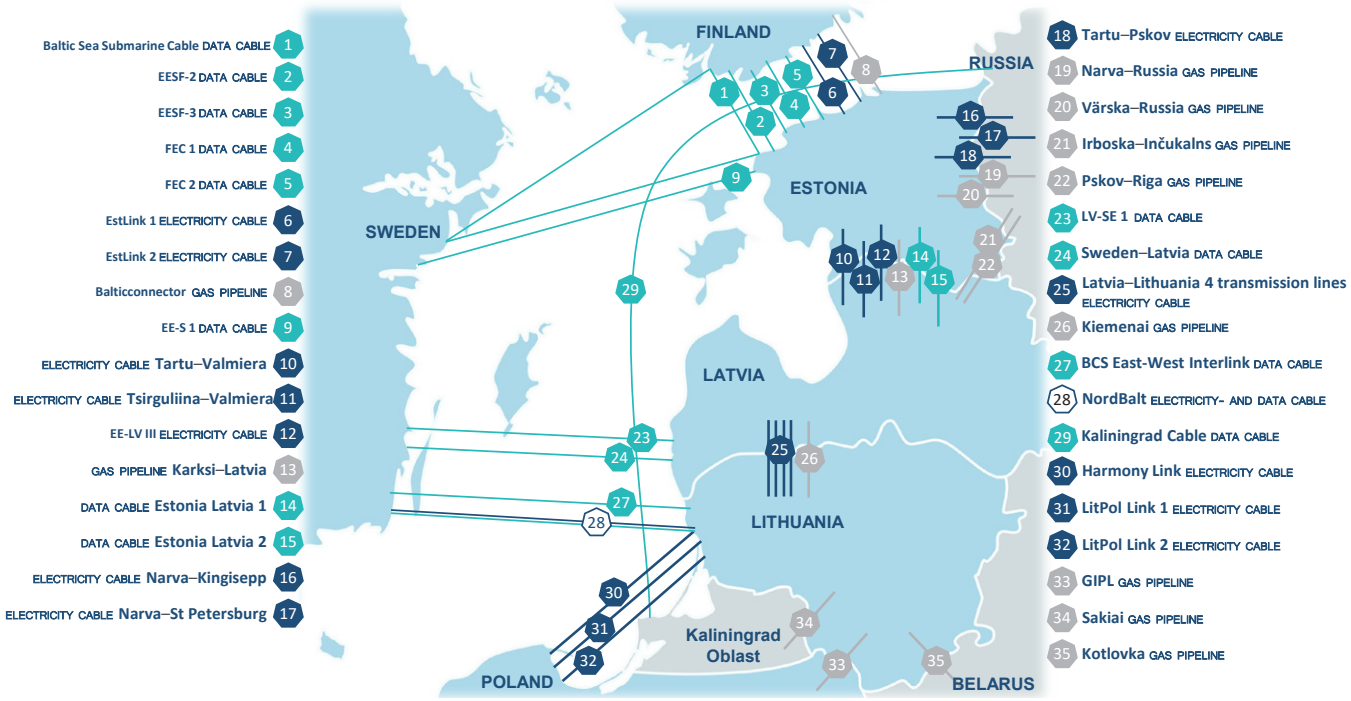


FIGURE 1. BALTIC STATES' AND KALININGRAD'S ENERGY AND DATA CONNECTIONS WITH NEIGHBORING COUNTRIES

1. ESTONIA'S ENERGY AND DATA CONNECTIONS WITH NEIGHBORING COUNTRIES

Estonia has 21 cross-border connections with neighboring countries, which ensure the daily provision of energy and data services (Figure 2). Ten of these connections are submarine cables. The seabed of the Baltic Sea hosts connections vital for the continuity of Estonia's critical services, linking the country to Finland and Sweden. Estonia is connected to Finland via five data cables, the Estlink 1 and Estlink 2 electricity cables, and the Balticconnector gas pipeline. Estonia also has two data cables linking it to Sweden.

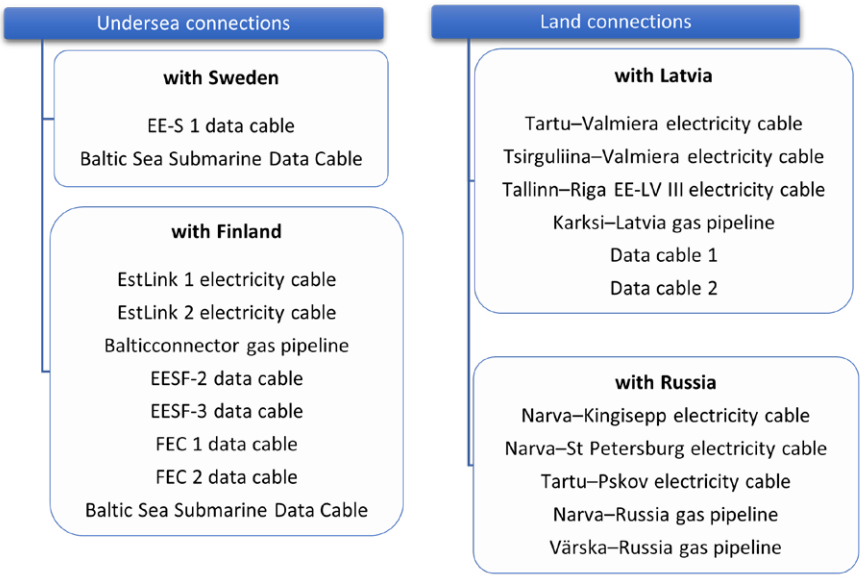


FIGURE 2. ESTONIA'S ENERGY AND DATA CONNECTIONS WITH NEIGHBORING COUNTRIES (COMPILED BY THE AUTHORS)

On land, Estonia has gas, electricity, and data connections with Latvia and Russia. Together, these established links form a network through which electricity flows not only to and from Estonia but also between Scandinavia, Latvia, and Lithuania, while gas is transported via pipelines between Lithuania, Latvia, and Finland. In the coming years,

Estonia plans to establish additional connections to meet the region's growing energy demands. Alongside new electricity connections with Finland and Latvia, the Nordic–Baltic Hydrogen Corridor is currently in the planning phase. This cross-border hydrogen infrastructure project running from Finland to Germany via the Baltic states and Poland is designed to connect regional hydrogen supply, demand, and storage (Elering, 2023a, pp. 67–68).

GAS

Estonia, Latvia, Lithuania, and Finland do not produce natural gas, which is why the entire region relies on imports from the global market. Estonia's gas transmission network has four cross-border connection points. Finland is linked to the Baltic and European gas systems and markets via the Balticconnector connection point in Paldiski. Balticconnector is also Estonia's only subsea gas supply connection. The connection to Latvia runs via the Karksi connection point on land. Estonia's land-based connections with Russia pass through the Narva and Värska connection points, though these have not been used since 2023. In response to Russia's aggression against Ukraine, the Estonian government decided on 29 September 2022 to impose sanctions on the import of natural gas and liquefied natural gas (LNG) from Russia, effective from 31 December 2022. As a result, gas trade with Russia has ceased (Elering, 2023b, p. 52) and is unlikely to resume soon (Elering, 2024b, p. 4). Estonia also facilitates land-based gas transit between Russia and Latvia. In southeastern Estonia, the Irboska–Inčukalns and Pskov–Riga parallel pipelines connect to Latvia at the Murati connection point and to Russia at the Luhamaa connection point (Elering, 2024b, p. 14), though these are not connected to Estonia's gas transmission network.

Previously, most of Estonia's gas supply came from Russia. Following the disruption of deliveries, connection points were established in 2022 to receive floating LNG terminals in Paldiski on the Estonian side and Inkoo on the Finnish side. Currently, all liquefied gas purchased on the global market is transported by ship to the Klaipeda LNG terminal in Lithuania or to the floating LNG terminal in Inkoo, Finland (Elering, 2023b, p. 19). These terminals are connected to the regional gas network, and gas reaches Estonia via the potential floating LNG terminal in Paldiski, from the Inčukalns underground gas storage facility in Latvia, from the Klaipeda LNG terminal in Lithuania, or from the Inkoo terminal in Finland via the Balticconnector connection. However, the Paldiski LNG terminal is only a backup solution, and its connection point can only be activated if a floating terminal with regasification capability is brought in (Elering, 2024b, p. 15). This means that its operation depends on ordering an LNG tanker and a regasification vessel.

The provider of gas transmission services in Estonia is Elering AS, which is responsible for transporting gas through the transmission network from the national border to customer connection points. Elering is also responsible for drafting contingency plans, which indirectly contribute to ensuring supply security and preventing emergencies in the gas system.

The completion of the Balticconnector in 2020 and the Gas Interconnection Poland–Lithuania (GIPL) in 2022 has integrated the Baltic and Finnish gas systems and markets with the rest of Europe. The construction of Balticconnector has been of critical importance for Estonia's supply security. It has eliminated the risk that, in the event of a major system failure, restrictions would need to be imposed on unprotected consumers (Elering, 2023b, p. 20). At the same time, the high level of integration in such a transmission network means that any major disruption would impact the entire regional gas system. In Estonia, the largest gas consumer is the energy sector. The gas network supplies reserve

power plants near Kiisa, which run on gas. Conversely, nearly all gas network equipment requires electricity to function (Elering, 2024b, p. 8). The primary power supply for gas equipment is provided through the electricity distribution network, while most backup power is ensured by auxiliary generators. The only exceptions are the Puiatu and Paldiski compressor stations.

According to Section 26[1] (2) ("Minimum requirements for supply security") of the Estonian Natural Gas Act (MGS), protected consumers are defined as follows: 1) household consumers whose installations are connected to the gas distribution network; and 2) energy companies that heat water for residential heating using district heating facilities that cannot operate on any fuel other than gas, and whose distribution networks—whether owned by or in possession of the company—cannot be supplied by a system using an alternative fuel. Section 26[1] (5) stipulates that gas supply disruptions caused by system failures must not exceed 72 consecutive hours and must not total more than 130 hours per year. The network operator is responsible for tracking the duration of such disruptions. The provider of gas transmission services in Estonia is Elering AS, which is responsible for transporting gas through the transmission network from the national border to customer connection points. Elering is also responsible for drafting contingency plans, which indirectly contribute to ensuring supply security and preventing emergencies in the gas system. At the national level, Elering prepares a "continuity risk assessment for critical services" and a "continuity plan for critical services" every two years (Elering, 2023b).

ELECTRICITY

Estonia has a total of eight cross-border electricity connections with neighboring countries. Two subsea direct-current cables (Estlink 1 and Estlink 2) connect Estonia to Finland; there are three land-based connections with both Latvia and Russia. Estonia is linked to Russia via three 330 kV transmission lines, two of which run from Narva to Saint Petersburg and Kingisepp, while the third runs from Tartu to Pskov. The Latvian electricity system is connected to Estonia through three 330 kV lines: Tartu–Valmiera, Tsirguliina–Valmiera, and Tallinn–Riga.

Until February 2025, the entire Baltic electricity system was synchronized with the Russian Integrated Power System / Unified Power System (IPS/UPS) frequency (see Figure 3), which was operated in a coordinated manner through the BRELL (Belarus, Russia, Estonia, Latvia, and Lithuania) cooperation agreement. To mitigate the risks associated with remaining within the Russian synchronous zone, all three Baltic states synchronized with the continental European frequency system in February 2025.

Between 2006 and 2016, the Baltic states made significant investments in additional subsea and land-based cables to build up supply security. The submarine cables between Estonia and Finland—Estlink 1 and Estlink 2—were completed in 2006 and 2014, respectively. In 2016, a submarine cable was put into operation between Lithuania and Sweden, while a land connection—LitPol Link—was brought into service between Lithuania and Poland in 2015. One of the last outstanding requirements for Estonia's future supply security is the construction of a submarine cable—HarmonyLink—between Lithuania and Poland, initially planned for completion in 2026. However, due to rising costs, a decision was made in 2023 to build HarmonyLink as a land-based connection instead (ERR, 2023a), with its completion now expected between 2028 and 2032, according to various sources (Elering, 2023a, p. 99; Skopljak, 2023).

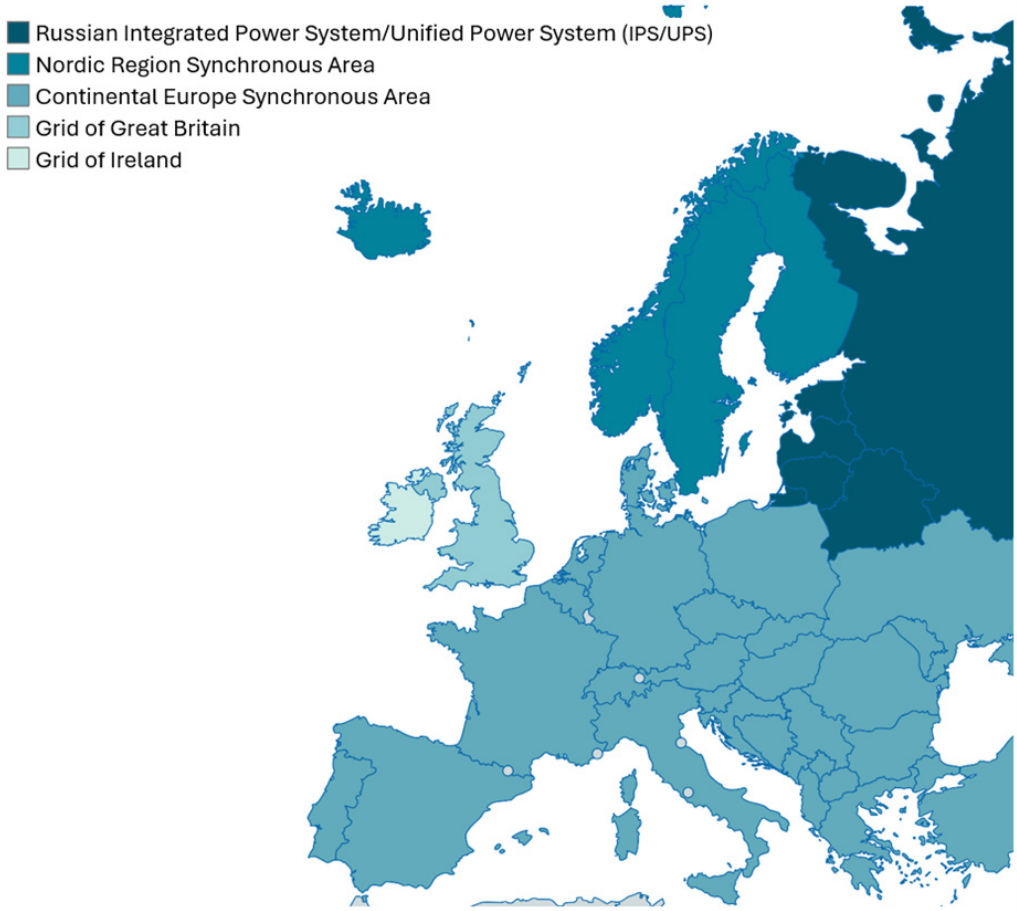


FIGURE 3. EUROPEAN ELECTRICITY SYSTEMS BEFORE FEBRUARY 2025 (SOURCE: ELERING, [N.D.], SUPPLEMENTED BY THE AUTHORS)

Estonia's electricity system is managed by Elering AS, which operates and develops the national transmission network as well as cross-border connections with Finland and Latvia. As the system operator, Elering is primarily responsible for ensuring unhindered electricity supply for Estonian consumers. Under Section 39 (7) and (8) and Section 66 (2), (3) and (4) of the Electricity Market Act, Elering is required to submit an annual supply security report statement and, under Section 14^1 of the Grid Code, conducts a system adequacy assessment. Under European Parliament Directive 2019/944 and Regulation 2019/943, the responsibility for evaluating and overseeing electricity grid reliability lies with organizations that are legally independent of system operators. In Estonia, this role is fulfilled by Baltic RCC OÜ, an entity established in 2022 and jointly owned by the Baltic states' system operators. Its tasks include the assessment of system adequacy, operational security, post-disturbance protocol, and the coherence of protection and recovery plans.

DATA

It is almost impossible to imagine modern life without data connections. Digital data is stored in data centers across different continents and transmitted globally through fiber-optic cables spanning land and oceans. Approximately 99% of the digital data that

influences our daily lives travels via undersea cables (Mauldin, 2023), including financial transactions between banks, emails, social media posts, and the exchange of information between various systems and control centers.

Estonia has a total of nine cross-border data connections. Two land-based cables link Estonia with Latvia, while the remaining seven are undersea cables. Estonia is connected to Finland by five and to Sweden by two submarine cables. The first undersea connections with Finland were established in 1992 and 1994, followed by a connection with Sweden in 1995. The three undersea cables are owned, in addition to Swedish and Danish companies, by Telia Eesti AS. Two additional cables to Finland, both completed in 2000, are owned by Elisa. The Baltic Sea Submarine Cable—which was completed in 2000 and connects Estonia, Finland, and Sweden—is owned by CITIC Telecom International, a company registered in Hong Kong (TeleGeography, 2024; CITIC Telecom International).

In Estonia, providing data communications is legally classified as a critical service, provided by various telecommunications companies. Under Section 2 of the regulation "Description and continuity requirements for critical telephone, mobile telephone and data communication services" (RT I, 26.02.2021, 17), these companies are required to plan, design, build, and maintain their communication networks in a way that will maximally shield them from any disruptive factors. Additionally, under Section 39(1) of the Emergency Act, telecommunications companies, as providers of critical services, are required to prepare continuity risk analyses and continuity plans to support continuity planning, risk assessment, and service restoration.

2. RISKS AFFECTING UNDERSEA ENERGY AND DATA CONNECTIONS

POTENTIAL CAUSES OF SERVICE DISRUPTIONS

Disruptions to critical infrastructure can have severe consequences for economic activity, social well-being, and national security (Pillai, 2023, p. 1). However, the security of critical services often fails to garner public attention until a breach occurs. It is only after serious incidents that the extent of dependence on this "invisible" network becomes fully understood. There are multiple threats that could lead to the disruption of subsea connections. Figure 4 shows a general breakdown of the causes of submarine cable damage worldwide, compiled since 1959.

Critical services' security often fails to garner public attention until a breach occurs.

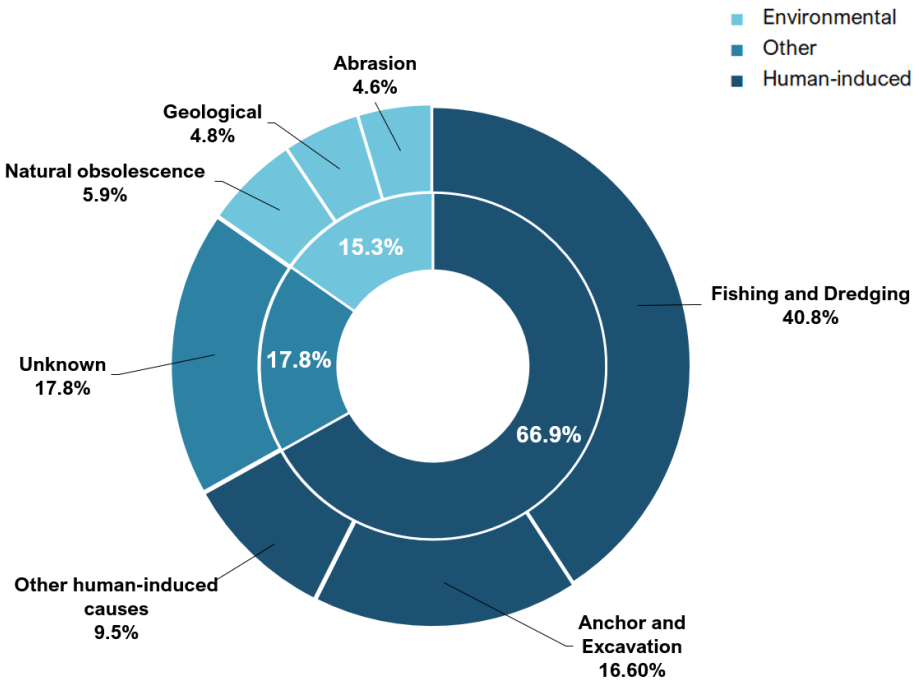


FIGURE 4. CAUSES OF SUBMARINE CABLE DAMAGE (COMPILED BY THE AUTHORS BASED ON CLARE, 2021)

Failures can result from system malfunctions, extreme natural events, or physical deterioration due to wear and tear. Human-induced causes, however, are the most common. Among these, it is important to distinguish between unintentional and deliberate causes. Accidental and unintentional damage may occur due to trawling or incorrect anchoring. By contrast, deliberate physical and cyberattacks targeting submarine cables, pipelines, land-based connection points, and control technologies are linked to sabotage or espionage.

The sabotage of critical infrastructure, including subsea infrastructure, can have various objectives. These may involve disrupting government communications or military command systems in the initial stages of an armed conflict, obstructing internet access, harming economic competitors, or causing supply disruptions, including for geopolitical purposes. Physical sabotage can also be deployed simultaneously (Wall & Morcos, 2021; Fridbertsson, 2023, p. 3) with other attack vectors, such as cyberattacks (Guilfoyle et al., 2022). This may form part of a broader hybrid warfare strategy designed to exploit a target's vulnerabilities, with a potentially extensive impact. For example, according to the UK's Ministry of Defense, as much as 99% of global internet traffic relies on submarine cables, while 77% of the UK's gas imports come from Norway via pipelines running beneath the North Sea (Brooke-Holland, 2023). Many NATO and European Union member states with maritime or oceanic coastlines experience similar dependencies on subsea infrastructure, leading to comparable vulnerabilities.

The sophistication of the methods used to damage critical infrastructure depends largely on the design of the network. For subsea connections, the underwater cable or pipeline is only one part of a larger system. Other vulnerable components include land-based connection points and control systems. As a result, deliberate damage to pipelines, cables, and connection points can range from simple physical attacks to sophisticated technology-driven hybrid assaults. Simpler methods involve using civilian vessels—such as fishing boats, and transport or research ships—to inflict damage on submarine cables and pipelines with anchors or trawling equipment. These types of attacks do not require advanced subsea technological capabilities and are relatively easy to carry out, even more so as civilian vessels do not attract significant attention in general maritime traffic (Bueger et al., 2022, p. 29). More complex attacks may involve submarines, underwater drones, divers, or explosive devices. In addition to physical destruction, land-based connection points and control systems may also be targeted using cyberattacks or a combination of both.

Deliberate damage to pipelines, cables, and connection points can range from simple physical attacks to sophisticated, multi-pronged hybrid assaults.

Each submarine cable or pipeline has at least two landing points where it connects to land-based infrastructure. For security reasons, the precise locations of these sites are often not publicly disclosed. However, multiple sources (including Bueger & Liebetrau, 2021; Frascà & Galantini, 2023; Insikt Group, 2023, p. 17; Bafoutsou et al., 2023, pp. 4, 19, 20, 30; Bueger et al., 2022, p. 29; Hendriks & Halem, 2024, p. 60; Schadlow & Helwig, 2020) indicate that these land-based connection points are the most vulnerable targets for deliberate attacks. This is primarily because landing stations are more accessible than deep-sea cables and pipelines, and even in developed economies, security at these facilities is often inadequate. Attack scenarios against cable landing points range from planned power outages to sabotage, espionage, or even explosive and missile attacks. Conducting attacks on land, including at connection points, is significantly cheaper and does not require the same level of specialist knowledge and equipment as subsea operations do.

In recent years, attacks aimed at severing cables in the Baltic Sea have been carried out using relatively simple and inexpensive methods, such as commercial vessels dragging their anchor across the seafloor. At the same time, it is evident that by conducting attacks in international waters, perpetrators seek to avoid the jurisdiction of affected states and to operate in a legal gray zone.

The continuous monitoring of subsea infrastructure is complex and resource-intensive, making it an attractive target for attackers, with cascading effects that can have long-term consequences.

Cyberattacks have also become a common component of infrastructure-targeting strategies. Cyberattacks can significantly disrupt data flows by hacking into network management systems used by private companies to control data traffic through cables. The worst-case scenario would involve a hacker gaining control of the network management system or obtaining administrator rights, enabling them to identify physical vulnerabilities in the system, disrupt or redirect data traffic, or execute what is known as a "kill click," which deletes the wavelengths used for data transmission (Wall & Morcos, 2021).

More complex than physically damaging or destroying submarine cables is tapping them to record, copy, and steal communication data to be analyzed for espionage and used for strategic purposes. Experts suggest that such operations can be carried out in three ways: inserting backdoors during the production process, targeting land-based stations, or directly tapping cables at sea (Wall & Morcos, 2021). This type of data espionage is not new—during the Cold War, US intelligence monitored a Soviet submarine cable as part of Operation Ivy Bells, which provided valuable insight into Soviet naval activities, processes, and technologies (Gehringer, 2023, p. 3). Strategic competition in underwater

EACH UNDERSEA CONNECTION HAS AT LEAST TWO VULNERABLE LANDING POINTS. PHOTOGRAPH: PIXABAY.COM

surveillance continues to evolve, with ongoing technological advancements aimed at securing strategic advantages.

Because the continuous monitoring of subsea infrastructure is physically and technically complex and highly resource-intensive, subsea infrastructure remains an attractive target for attackers, with cascading effects that can have long-term consequences. Identifying weak points in subsea infrastructure and carrying out repairs is a time- and resource-intensive process. The time required to repair damage to submarine cables and their land-based connection points depends on various factors, including the identification of the fault location, the availability of repair vessels, and the supply and accessibility of the necessary components and materials. Due to the excessive cost and technical specificity of the equipment involved, only a limited number of companies worldwide specialize in the maintenance and repair of subsea connections. Specialist repair vessels are also in short supply globally (Bafoutsou et al., 2023, p. 4), and their arrival at the site of a failure may take considerable time. Additional factors include weather conditions and the process of obtaining special permits to authorize repair work in specific waters. In many cases, even identifying the precise location of a fault can take weeks. A notable example is the Estlink 2 failure in January 2024, where the search for the fault location took more than a month (ERR, 2024a). Furthermore, the availability and accessibility of components required for restoring or replacing damaged connections, as well as the complexity of the repair process, directly impact the duration of restoration efforts. The extended repair times of both Estlink 2, which took more than seven months to fix, and Balticconnector, which required six and a half months, have underlined a critical risk: restoring critical connections may take more than six months.

TAPPING UNDERSEA CABLES IS A METHOD TO STEAL COMMUNICATIONS DATA. PHOTOGRAPH: PEXELS.COM

Both the Estlink 2 and Balticconnector failures have highlighted a significant vulnerability: restoring critical connections may take more than six months.

UNDERSEA INFRASTRUCTURE AS A STRATEGIC INTEREST FOR RUSSIA AND CHINA

Protecting subsea connections from attack is increasingly becoming a challenge, as rapid technological advancements provide aggressors with ever-greater advantages. Numerous sources highlight the extensive efforts of Russia and China to survey subsea infrastructure and develop sabotage capabilities, which form a key part of their ongoing economic and geostrategic competition with the United States and the European Union (see, e.g., Burdette, 2021; Bueger et al., 2022; Gehringer, 2023; Insikt Group, 2023; Kaushal, 2023; Kumar, 2023; Nakamura, 2023; Scott, 2022; Siebold, 2023; Ten Houten, 2023; Janda & Corera, 2024; Loik, 2024). Several sources (see, e.g., Roy, 2018; CCDCOE, 2019; Geri, 2023; Long, 2023) also

The main threat to Europe's submarine cables originates from Russia. Moreover, cooperation between Russia and the People's Republic of China in this area has intensified.

emphasize the strategic goal of competing states to achieve an informational advantage—ideally dominance—through the control of subsea communications infrastructure and to improve their cyberattack capabilities against rivals.

Russia has shown an increasing willingness to use its capabilities for unconventional and hybrid attacks.

The main threat to Europe's submarine cables stems from Russia (Frascà & Galantini, 2023, p. 59), which has gained extensive experience over the years and is prepared to use its naval capabilities aggressively to disrupt communication networks (Wasiuta, 2023, p. 367). Russian hybrid tactics pose an acute threat to critical subsea infrastructure in Northern Europe (Monaghan et al., 2023, p. 2), the Atlantic Ocean, the Black Sea, and other regions. Targeting critical infrastructure is reportedly a key component of Russia's military doctrine, and as the war in Ukraine is likely to engage its conventional forces for several more years, Russia seeks to gain asymmetric advantages in strategically significant areas such as subsea infrastructure. The maritime domain is an integral part of both Russia's naval doctrine and the operational structure of its military's and intelligence services' maritime operations (Hendriks & Halem, 2024, pp. 7, 10, 26). A significant increase in Russian naval activity near subsea communication cables was observed after the annexation of Crimea in 2014, followed by the expansion of its invasion into eastern Ukraine and its intervention in the Syrian civil war in 2015 (Sanger & Schmitt, 2015). Many sources also indicate that Russia has demonstrated an increasing readiness to use its capabilities for unconventional and hybrid attacks (see, e.g., Bueger et al., 2022; Hendriks & Halem, 2024; Siebold, 2023; Cooper, 2023; Frascà & Galantini, 2023; Wasiuta, 2023; Loik, 2024). NATO and EU member states must therefore enhance their mutual intelligence-sharing and develop integrated monitoring and defense measures.

One scenario discussed within NATO is the possibility that Russian submarines could prepare to sever submarine cables in the Atlantic Ocean. Given that approximately 97% of communication between the United States and Europe passes through these submarine cables, their destruction could have severe consequences. According to Brzozowski (2020), such attacks could be part of hybrid warfare. The U.S. Intelligence Community's 2024 Annual Threat Assessment also emphasizes that "Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries." (Annual Threat Assessment, 2024, p. 16).

British and American military officials have repeatedly warned that Russia possesses the technical expertise to sabotage parts of the world's subsea internet infrastructure, including the digital networks of several Western states (Scott, 2022). The Main Directorate of Deep-Sea Research (*Главное управление глубоководных исследований*, GUGI), a part of the Russian Ministry of Defense, is known to have access to spy ships, specialist submarines, and the capability to deploy aquanauts, mini-submarines, or underwater drones. In 2018, Russia was reportedly working on 17 underwater drone projects. Possible attack methods include detonating torpedo warheads or placing remotely activated mines (Ten Houten, 2023). Although GUGI is a classified unit that operates independently from other branches of the armed forces, its vessels and personnel have been linked to various units of the Russian Navy. For example, during the final phase of Nord Stream 2 construction (from 10 April to 30 August 2021), reports emerged of Russian naval personnel operating in the construction area. A special-purpose unit was observed aboard civilian vessels of the Russian Marine Rescue Service. Members of this joint unit were identified as belonging to various Russian naval special forces units (data from Ryzhenko, 2022): four members from GUGI, seven from the 313th Special-Purpose Detachment for Com-

bating Underwater Sabotage of the Baltic Fleet, and seven from the 342nd Emergency Rescue Detachment of the Baltic Fleet.

One of the vessels supposedly used by GUGI is the *Yantar*, a so-called "specialist oceanographic research vessel," which has been observed periodically around the world, from the Caribbean Sea to the Persian Gulf, as well as near subsea infrastructure off the coast of Ireland. Equipped with submersibles capable of operating at depths of up to 6,000 meters, the *Yantar* has been suspected of conducting surveillance on submarine infrastructure and equipment, including submarine cables and underwater sensors. Additionally, Russia's Naval Intelligence Directorate possesses resources capable of carrying out espionage and sabotage operations under the command of Russia's military intelligence (GRU) (Nakamura, 2023). In April 2023, Swedish, Danish, Norwegian, and Finnish broadcasting organizations published a report that tracked Russian naval activities in the North Sea. This included monitoring the *Admiral Vladimirsky*, a vessel believed to be engaged in maritime reconnaissance, which was observed sailing near offshore wind farms. Individuals aboard the ship were seen wearing face masks, ballistic vests, and carrying automatic weapons.

The broadcasting organizations involved in the investigation used various data analysis techniques, intercepted radio communications, and intelligence sources, which confirmed that approximately 50 separate Russian vessels had gathered intelligence in the North Sea over the past decade. Their intelligence-gathering efforts involved using underwater surveillance devices to map key locations for potential sabotage (Corera, 2023; Fastrup et al., 2023; Hou et al., 2023). The above examples demonstrate both Russia's active interest in and its operational capability to monitor, disrupt, and, if necessary, damage NATO and EU countries' critical underwater infrastructure. The existence of these capabilities, alongside the continuous monitoring of the region, underlines the necessity of maintaining oversight of vessels that remain in critical areas of interest for extended periods.

Numerous examples confirm both Russia's active interest in and its real capability to monitor, disrupt and, if necessary, damage NATO and EU countries' critical underwater infrastructure. This activity is being carried out with increasing cooperation from the People's Republic of China.

The Baltic Sea has also seen the repeated damaging of subsea infrastructure in which Russian involvement has either been confirmed or strongly suspected. For example, in the first half of 2015, Russian vessels repeatedly damaged the NordBalt cable linking Lithuania and Sweden. This 400-kilometer-long cable runs from Klaipeda to Nybro and enhances electricity supply security in both the Nordic region and Lithuania. Russia responded to the Swedish and Lithuanian governments' accusations by claiming that its actions were intended to protect the country's "military exercise zone" (Euractiv, 2015). Such hostile activities are typically conducted in a manner that ensures plausible deniability, creating the impression of an accident to mislead investigations. The Russian Navy, for example, has used regular maintenance and repair work on the Nord Stream pipelines as a convenient cover for reconnaissance and sabotage activities in the Baltic Sea (see, e.g., Ryzhenko, 2022). Russian naval and associated vessels have also been active near critical infrastructure belonging to Norway, the United Kingdom, the Netherlands, Belgium, and other NATO and EU member states in both the North Sea and the Baltic Sea (see, e.g., Page, 2023; Pillai, 2023, p. 5), indicating an increased intelligence focus as well as possible activities in preparation for sabotage operations.

China's activities are primarily focused on cable production, installation, and investment to secure control over global data flows.

In connection to the destruction of Estlink 2 as well as several data cables in December 2024, concerns have been raised about threats posed by Russia's shadow fleet. The vessel *Eagle S*, which was involved

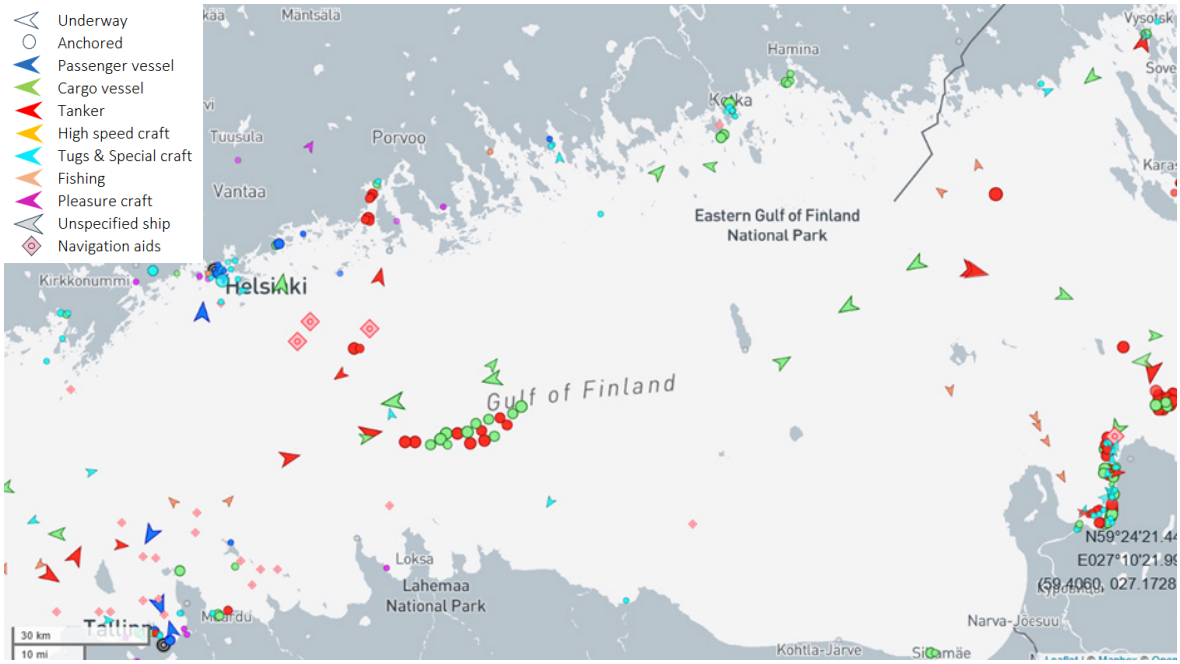


FIGURE 5. ANCHORED TANKERS AND CARGO SHIPS SUSPECTED TO BE MEMBERS OF RUSSIA'S SHADOW FLEET IN THE GULF OF FINLAND, 15 JANUARY 2025 (SOURCE: MARINETRAFFIC.COM)

in the December 2024 incident, has been identified as a possible member of this shadow fleet (Milne, 2024). The Russian shadow fleet consists of tankers transporting Russian crude oil and petroleum products at prices above the $60-per-barrel global oil price cap imposed on Russian crude by the G7 and the EU in December 2022. As the G7's and the EU's decision prohibited insurance companies in their member states from insuring tankers carrying Russian oil sold above the price cap, Russian shadow fleet tankers operate without valid (non-Russian) insurance. Most of these vessels also disable their automatic identification system (AIS) to obfuscate their movements. The owners of shadow fleet vessels are mostly shell companies based in Hong Kong or the United Arab Emirates. These tankers rarely sail under the Russian flag, with their registered home ports typically located in Africa or in the Pacific.

The suspicion that *Eagle S* is part of the shadow fleet is justified, as the vessel lacked valid insurance at the time of its seizure by Finnish authorities, and its S-band radar was non-operational. However, *Eagle S* did have a functioning AIS system, which allowed Finnish authorities to confirm its presence over Estlink 2 at the time of the incident (Maritime Executive, 2025; de Keyserling, 2023; Katinas & Wickenden, 2024; Bockmann, 2024; Bouisso, Michel & Tchoubar, 2024; Katinas, 2024; Levi, 2024; Raghunandan, 2024a, 2024b; Stognei, 2024; Stuart, 2024).

Until the arrest of the *Eagle S* in December 2024, the primary concern regarding the shadow fleet was the environmental risk it posed to the sea and coastal states. The shadow fleet's uninsured vessels are generally in poor condition, and offshore ship-to-ship oil transfers, which form an integral part of the shadow fleet's modus operandi, pose a considerable pollution hazard. In January 2024, a vessel sailing under the Liberian flag and carrying Russian oil to Türkiye broke down in the Bosporus, disrupting maritime traffic for hours. In December 2024, an oil spill occurred in the Black Sea after two Russian tankers, the *Volgoneft' 212* and the *Volgoneft' 239*, became damaged during a storm. The *Eagle S* case is, however, the first known incident in which a likely shadow fleet tanker is suspected of deliberately sabotaging submarine infrastructure, thus adding a new threat

posed by the shadow fleet to EU and NATO members. To date, the EU has identified 79 shadow fleet tankers in its sanctions packages. In total, 118 tankers have been sanctioned by the EU, the US, and the UK, though only three vessels have been subject to sanctions from all three entities simultaneously. The Ukrainian government estimates the shadow fleet to comprise more than a thousand vessels. Tellingly, neither the *Eagle S* nor its owner was under EU, UK, or US sanctions at the time of the Estlink 2 disruption (Anadolu Agency, 2024; Gavin, 2024; Katinas & Wickenden, 2024; Shadow Fleet, [n.d.]; Reuters, 2024).

The latest suspected Russian attacks on subsea infrastructure, carried out using civilian vessels, point toward the involvement of intelligence services rather than the direct use of naval forces. As several incidents detailed in this report indicate, Russian cooperation with the People's Republic of China is being facilitated through various intermediaries. There are multiple signs of strengthening military ties between Russia and China: as of July 2024, Russia and China had participated in more than 102 joint military exercises since 2017, including anti-submarine warfare drills in the Pacific Ocean (Green, 2024). Further evidence of the deepening strategic cooperation between Russia and China at sea is the Ocean-24 joint naval exercise, conducted in September 2024. This exercise spanned the Pacific Ocean, the Arctic Ocean, and the Mediterranean, Caspian, and Baltic Seas, reportedly involving approximately 400 warships, submarines, and support vessels, over 120 aircraft and helicopters, and an estimated 90,000 military personnel (Associated Press, 2024).

Russia has kept its own dependence on subsea infrastructure relatively minimal, maintaining connections to the global data transmission network through only four international submarine cables—one linking it to Finland, one to Georgia, and two to Japan. According to Gehringer (2023, p. 5), this limited number of connections allows Russia to maintain tight control over its landing points and data traffic. In contrast, China's approach to subsea infrastructure is more tactical, focusing on cable manufacturing, installation, and investment in critical infrastructure to gain control over global data flows and secure a competitive edge in strategic sectors over other major powers.

Alongside Russia, the People's Republic of China represents the greatest threat to intercontinental data cables and their infrastructure. China is aggressively expanding its presence in the submarine cable sector worldwide to consolidate its influence over global data and information flows (Curtis & Rasser, 2021, p. 5). A prominent example of growing economic and geostrategic competition, as cited by Gehringer (2023), is PEACE (Pakistan East Africa Connecting Europe), which forms part of the Digital Silk Road. This 15,000-kilometer-long submarine cable connects Pakistan to Western Europe via the Horn of Africa, the Red Sea, and the Suez Canal, with its landing point in the French coastal city of Marseille. At the same time, connections are being built in East Africa, linking Somalia to Kenya. In 2017, China established its first overseas military base in Djibouti, a country situated on the Red Sea. Djibouti also serves as a landing site for numerous submarine cables connecting Asia and Europe.

As part of its national strategic plan, Made in China 2025, the Chinese Communist Party has set a goal of capturing 60% of the global fiber-optic cable market, while simultaneously asserting that submarine cable installation is not merely a business venture but also a battlefield for information acquisition (Kuszynski & Barns, 2022, p. 9). For example, the Chinese company Hengtong Optic-Electric is one of the world's largest fiber-optic glass manufacturers, while another Chinese firm, HMN Tech (formerly Huawei Marine Networks), has installed and currently maintains a quarter of the world's submarine cables. The European Parliament has expressed deep concern (European Parliament, 2024) over

A major risk lies in the submarine cable system managed by HMN Technologies, which is designated for data transmission and connects EU member states with the Indo-Pacific region. This includes links to NATO military bases, raising cybersecurity, underwater surveillance, data protection, and intelligence-gathering vulnerabilities.

the fact that diplomatic and military communications within the EU and its member states rely on privately owned submarine cables manufactured by Chinese companies, such as HMN Technologies, which are linked to the People's Liberation Army's cyber intelligence units. A major risk lies in the submarine cable system managed by HMN Technologies, which is designated for data transmission and connects EU member states with the Indo-Pacific region. This includes links to NATO military bases, raising cybersecurity, underwater surveillance, data protection, and intelligence-gathering vulnerabilities.

The European Parliament (2024, point 9) has also highlighted that the backbone of Estonia's internet infrastructure, formerly owned by a Dutch company, was sold to a Chinese company linked to the People's Liberation Army. It stresses the need for joint efforts among member states to prevent similar cases in the future.

The security of subsea connections running through the Baltic Sea, both for the Baltic states and other coastal countries in the region, is further complicated by the presence of Russia's Kaliningrad Oblast, located between Lithuania and Poland. This gives Russia military leverage in the Baltic Sea, as its only other access to the waterway is in the far eastern corner of the peripheral Gulf of Finland. Kaliningrad's location on the Baltic Proper enhances Russia's capacity for destabilizing activities across the entire sea. Kaliningrad is thus of exceptional strategic importance to Russia, as losing control over the exclave would severely diminish its capabilities in the Baltic region (*Известия*, 2024). However, Kaliningrad is also a liability for Russia, as in the event of a conflict, Moscow would face significant challenges in defending it.

Before Sweden joined NATO, Kaliningrad's territorial waters and exclusive economic zone effectively severed NATO-controlled waters in the Baltic, which would otherwise have formed a continuous corridor from Denmark to Finland. Even after Sweden's accession, Kaliningrad's territorial waters and economic zone remain adjacent to those of NATO member states, providing Russia with the ability to monitor and interfere with maritime activities there. Furthermore, should Belarus's Moscow-aligned regime remain in place, Kaliningrad will enable Russia to maintain strategic pressure on the Baltic states indefinitely, potentially cutting off the Suwałki Corridor, as well as threatening Poland from both the north and the east (see Rozhkov-Yuryevsky, 2013, p. 122; Żyła, 2019, pp. 102–103; Veebel, 2019, pp. 193–195).

Due to geographical constraints, Kaliningrad's subsea connections to the rest of Russia are extremely limited. The most significant link is the Baltika fiber-optic cable, a 1,115-kilometer cable opened in 2021, which links the exclave to Leningrad Oblast and thus to Russia's broader data network. The cable also provides Russia with a potential pretext for covert operations in the Baltic Sea. Following the suspected sabotage of multiple communication cables and the Balticconnector gas pipeline on 7 and 8 October 2023, allegedly carried out by the cargo ship *Newnew Polar Bear*, the first vessel to arrive in Finland's exclusive economic zone for repairs was the Russian salvage ship *Spasatel' Karev*.

The failure of Baltika in October 2023 is a significant case. On the one hand, the damage could be explained by the general destruction caused by *Newnew Polar Bear*, a Hong Kong-flagged cargo ship, which was dragging its allegedly forgotten anchor along the seabed. On the other hand, Swedish state media have highlighted that, in addition to the *Newnew Polar Bear*, the Russian nuclear-powered container ship *Sevmorput'*, owned by the state corporation Rosatom, was also present in the same area at the time of the inci-

dent. *Sevmorput'*, which can also function as an icebreaker capable of cutting through ice up to one meter thick (ROSATOM FLOT, 2012), was near *Newnew Polar Bear* on 7 and 8 October (Granlund & Velizelos, 2023). Therefore, it cannot be ruled out that the damage to Baltika served as a smokescreen for a joint Russo–Chinese operation against Balticconnector, FEC, and EE-S1. This hypothesis is further supported by the connections of *Newnew Polar Bear*'s owner, as well as the ship's movements before and after the incident.

Newnew Polar Bear's owner, Yangpu NewNew Shipping, was incorporated in Hong Kong in 2023 and acquired the vessel in June of that year. Although the company's stated objective, according to its Russian representative Ke Jin, is to provide regular container services from southern Chinese ports to Arkhangelsk, Saint Petersburg, and Kaliningrad via the Northern Sea Route, analyst Tan Hua Joo from Linerlytica has noted that the company's ships lack the necessary ice classification for safely navigating the route. Rosatom's representative, Vladimir Panov, has confirmed that Rosatom, which oversees all Russian nuclear icebreakers, ensures escort services for Yangpu NewNew Shipping's vessels (Interfax, 2023; Li, 2023). Thus, Yangpu NewNew Shipping has direct ties to a Russian state enterprise, making *Sevmorput*'s presence near *Newnew Polar Bear* theoretically justifiable as part of contractual obligations between the parties.

Kaliningrad Oblast is a strategically critical region for Russia, without which it would lose most of its strategic and operational capabilities in the Baltic Sea.

Additionally, Yangpu NewNew Shipping is not the only entity authorized to negotiate contracts related to *Newnew Polar Bear*. Rosatom is also responsible for issuing permits required for vessels navigating the Northern Sea Route. While Rosatom granted *Newnew Polar Bear* permission to traverse the Northern Sea Route between 15 July and 31 October 2023 at the request of Yangpu NewNew Shipping, a subsequent permit for the ship to use the route from 1 to 15 November 2023 was issued at the request of the Russian company OOO Torgmoll (NSR General Administration ROSATOM, 2023a; 2023b). The Russian–Chinese Business Council (Российско-Китайский Деловой Совет)—whose co-chairs are Kremlin-affiliated oligarch Gennady Timchenko and Ren Hongbin, head of the China Council for the Promotion of International Trade (CCPIT), an entity under China's Ministry of Commerce—lists OOO Torgmoll as part of China's One Belt, One Road investment strategy (Aoyama, 2016, pp. 4–7; Postimees, 2016; China Council for the Promotion of International Trade CCPIT, 2024; Российско-Китайский Деловой Совет, 2024a; 2024b).

Beyond the suspicious ownership structures, *Newnew Polar Bear*'s trajectory before and after the damage to the communication cables and gas pipeline on the evening of 7 October and early morning of 8 October 2023 also raises concerns. On 3 October, the ship arrived at the port of Kaliningrad, and on 6 October, it docked in Baltiysk, home to the largest naval base of Russia's Baltic Fleet. On 8 October, *Newnew Polar Bear* reached Saint Petersburg, only to depart again for Kaliningrad—contrary to maritime law, which states that a vessel that has lost its anchor should not be deemed seaworthy. *Newnew Polar Bear* then returned to Kaliningrad on 13 October (MarineTraffic.com, 2024). Considering the ownership of *Newnew Polar Bear*, the ship's behavior before (departing from the Baltiysk naval base in Kaliningrad Oblast, pairing with *Sevmorput'*, a nuclear-powered icebreaker operated by a Russian state enterprise) and after the infrastructure damage (sailing back to Kaliningrad from Saint Petersburg without an anchor), and the unusually swift repair of Baltika, it cannot be ruled out that *Newnew Polar Bear*'s activities were part of a preplanned operation. In this scenario, the subsea infrastructure between Leningrad Oblast and Kaliningrad Oblast—and its alleged damage—served as a cover for the operation.

It cannot be ruled out that the damage to Baltika served as a smokescreen for a joint Russian–Chinese operation against Balticconnector, FEC, and EE-S1.

3. PLANNED RISK MITIGATION MEASURES AND THEIR ADEQUACY CONSIDERING HEIGHTENED SECURITY THREATS

INCIDENTS THAT HAVE AFFECTED ESTONIA'S AND ITS NEIGHBORING COUNTRIES' SUBSEA CONNECTIONS IN THE PAST THREE YEARS

Although most deliberate attacks on subsea connections are intended as demonstrations of power or provocations aimed at exposing the vulnerability of such infrastructure for various states, the potential damage from larger-scale attacks poses a significant risk to the continuity of critical national services.

Based on disruptions to subsea connections across different regions of Europe over the past three years, it is clear—even in the absence of officially confirmed data—that the number of deliberate human-induced incidents targeting subsea infrastructure in the region has increased. Since 2021, eight suspicious cable breakage incidents have occurred in the Euro-Atlantic area, along with over 70 publicly reported cases of Russian vessels behaving unusually near critical maritime infrastructure (Hendriks & Halem, 2024, p. 10). More recent incidents in November and December 2024 and in January 2025 are currently still under investigation.

In April 2021, Norway reported damage to a submarine cable connecting it to the Lofoten-Vesterålen ocean observatory in Svalbard. A 4.2-kilometer section of the fiber-optic cable, equipped with underwater sensors, was found to be missing (Kirk, 2022). In November, Norwegian authorities located the severed cable segment 11 kilometers from its original position, outside Norway's economic waters. This cable was capable of tracking submarine movements and was in a passage frequently used by Russian naval forces traveling from Murmansk to the Atlantic Ocean (Tammepuu, 2023). There is reason to suspect that this was a deliberate act of Russian sabotage (Newdick, 2021). In January 2022, one of the two submarine cables connecting Norway to Svalbard was severed. The disruption is suspected to have been caused by human activity, with reports pointing to Russia as a likely perpetrator, given its known capabilities in conducting such sabotage operations (Humpert, 2022). Journalists from Norway's national broadcaster

FIGURE 6. MAP OF SUBSEA CONNECTION DISRUPTIONS IN THE BALTIC SEA IN RECENT YEARS

NRK tracked the movement of a Russian fishing trawler 20 times over the broken cables in the days before and after the damage occurred (Kirk, 2022).

In September 2022, explosions occurred along the Nord Stream gas pipelines in the exclusive economic zones of Denmark and Sweden. According to Swedish prosecutors, investigators found traces of explosives near the damaged sites, confirming that the incident was an act of sabotage (Ringstrom & Solsvik, 2022). In October 2022, three communication cables near a subsea landing station off the coast of France were severed. The cause of the damage was linked to vandalism or sabotage (Brussels Times, 2022). The following day, communication between the Shetland Islands and Scotland was disrupted after a submarine cable failure, which followed the severing of another subsea communication cable between Shetland and the Faroe Islands a week earlier (BBC, 2022). During this period, Russian vessels were repeatedly observed in the affected areas (Hendriks & Halem, 2024, p. 10).

In October 2023, the Balticconnector gas pipeline between Estonia and Finland, as well as subsea communication cables between Estonia and Sweden and between Estonia and Finland, were severed in the Baltic Sea. The gas pipeline leak took place in Finland's exclusive economic zone. At the same time, a communication cable linking Finland and Estonia was damaged, and the previous day, a cable linking Estonia to Sweden was also affected, with the damage occurring approximately 50 kilometers offshore west of Hiiu-

The number of deliberate, human-induced incidents targeting subsea infrastructure has increased in the Baltic Sea region.

maa. Following these events, Finnish President Sauli Niinistö issued a statement confirming that the disruptions were caused by external activity (Tanner, 2023). According to Finnish foreign and security policy sources, the Finnish government considers it likely that the incident was a case of Russian sabotage (ERR, 2023b). The gas pipeline and cables are suspected to have been damaged by the anchor of *Newnew Polar Bear*, a Hong Kong-registered vessel en route from Kaliningrad to Saint Petersburg (ERR, 2024b). NATO Secretary-General Jens Stoltenberg also issued a statement on the incident, emphasizing that if the damage to the gas pipeline and communication cable was a deliberate attack on critical infrastructure, it would be regarded as a profoundly serious incident requiring a unified NATO response (Postimees, 2023). On 12 August, Hong Kong media reported that, following an internal investigation, Chinese authorities admitted that the Balticconnector gas pipeline had been accidentally damaged, attributing the incident to a severe storm (ERR, 2024e). As of the end of 2024, the investigation remains ongoing. The connection was restored on 22 April 2024.

On 17 November 2024, two subsea communication cables in the Baltic Sea were severed—the BCS East-West Interlink between Sweden and Lithuania and the C-Lion1 cable between Finland and Germany. Preliminary information indicated that the damage was linked to the Chinese-flagged cargo vessel *Yi Peng 3*, which had departed from the Russian port of Ust-Luga and was owned by the Chinese company Ningbo Yipeng Shipping Co. LTD (Madsen, 2024). No state has officially confirmed sabotage, and Russian authorities have denied any involvement in the cable disruptions. However, according to government sources involved in the investigation, Russian intelligence provided instructions to the captain of *Yi Peng 3* to use an anchor to cut through the communication cables (Pancevski, 2024). Both connections were restored within two weeks.

On 25 December 2024, the Estonia–Finland electricity cable Estlink 2 was severed. That same evening, the Estonian Consumer Protection and Technical Regulatory Authority received information that three additional subsea communication cables between Estonia and Finland had been affected—two cables owned by the Elisa Group had been severed, while a CITIC Telecom cable had sustained damage (Lomp, 2024). The primary suspect was the *Eagle S*, a Cook Islands-registered oil tanker that had departed from Ust-Luga, Russia, on the morning of 25 December. The vessel is owned by Caravella LLC FZ, a company based in the United Arab Emirates (UAE), and is believed to be part of Russia's shadow fleet (Yle, 2024). Unlike previous cases, where vessels suspected of involvement were merely flagged for further inquiry by their country of registration (as in the *Newnew Polar Bear* case, ERR, 2023d), the Finnish Border Guard escorted *Eagle S* into Finnish territorial waters (Yle, 2024). The vessel was subsequently seized by the Finnish National Bureau of Investigation and the Border Guard for investigative procedures (Sajari, 2024). It was detained and placed at the Svartbäck oil terminal in Porvoo (Kressa, 2024). This intervention is believed to have prevented the potential destruction of Estlink 1 and the Balticconnector gas pipeline (Kivi, 2024).

Many sources indicate that the likelihood of attacks against critical subsea infrastructure is increasing, which makes it crucial to introduce regulatory corrections as swiftly as possible and implement additional physical security measures.

The detention was justified primarily on two grounds: first, states have the right to inspect vessels entering their territorial waters to ensure they are in a seaworthy condition; second, inspections can be conducted to determine whether a vessel has engaged in sabotage (Alandi, 2025). Based on these considerations, Finnish authorities proceeded with the seizure of the vessel.

On 26 January 2025, a fiber-optic data cable between Sweden and Latvia in the Baltic Sea was damaged. The cable was severed in

Sweden's exclusive economic zone, and the main suspect is the vessel *Vezhen*, sailing under the Maltese flag and owned by the Chinese government (ERR, 2025). The ship had started its last voyage from the port of Ust-Luga in Russia and was detained by the Swedish Security Service (Säpo) due to a missing anchor fluke. The vessel has been seized, and the Swedish Prosecution Authority has launched an investigation into aggravated sabotage (Kulleste, 2025). From the listed incidents, unconfirmed reports suggest an escalation of geopolitical tensions manifesting in provocations aimed at causing damage to Western states. However, due to regulatory gaps in legislation governing the protection of long-distance subsea energy and data connections, determining the motives and perpetrators of such incidents remains speculative. According to multiple sources (Council of Europe, 2024; Hendriks & Halem, 2024, pp. 15, 23, 27, 29; Pleasic, 2024, p. 17; Insikt Group, 2023, p. 5; Frascà & Galantini, 2023, p. 15; Wasiuta, 2023, p. 363; Radin, 2017, p. 13), the likelihood of such attacks increasing in the coming years is high. This underlines the need for urgent regulatory adjustments and the implementation of additional protective measures.

However, in addition to regulatory amendments, existing regulations must also be enforced more assertively. In 2023, following the Balticconnector gas pipeline rupture and the severing of the Finland–Germany submarine cable in 2024, the prevailing rhetoric was that little could be done (ERR, 2024g). However, by the end of 2024, Denmark had detained a vessel responsible for damaging submarine cables (ERR, 2024f). This stance persisted even after Denmark had already apprehended the suspect vessel. On 25 December 2024, when *Eagle S* severed Estlink 2, police and border guard special forces were deployed onto the vessel, and it was directed to a Finnish port. All these incidents occurred under similar legal conditions, with no interim changes to the law of the sea, yet the state responses varied significantly.

On 9 January 2025, the Estonian government decided to submit a draft amendment to the Estonian Penal Code to Parliament, proposing penalties for infrastructure damage occurring outside Estonia's territorial waters (Justiits- ja digiministeerium, 2025). However, the necessity of this amendment remains questionable, as the existing provisions on territorial applicability in the Penal Code already extend to such instances. For example, the same territorial applicability has previously been used in criminal proceedings related to offenses committed in Afghanistan (Kaitsepolitseiamet, 2009, p. 23) and for legal actions in Africa. In 2006, the tanker *Flawless* was suspected of causing maritime and coastal pollution in Estonian waters and was subjected to legal proceedings outside Estonia's territorial waters (Prokuratuur, 2006). Any clarification of legal applicability may also have implications for past cases, such as the investigations into the Balticconnector incident and the simultaneous severing of the communication cable.

IMPACT OF ENERGY AND DATA DISRUPTIONS ON THE CONTINUITY OF ESTONIA'S CRITICAL SERVICES

All the threats listed above apply to Estonia's energy and data connections to neighboring countries. The primary risk to the continuity of critical services is the disruption of basic services such as electricity supply, heating, and data transmission due to interruptions in energy and data connections. The risk level associated with natural processes in Estonia is low, and environmental issues or weather phenomena (storms, tides, etc.) rarely cause significant disruptions, except for frequent interruptions in overhead power lines. Wear and tear and technological failures are more common. Although rare, such incidents

For the Baltic states, in addition to possible disruptions in data connections, a significant risk factor lies in the subsea electricity and gas pipelines running along the Baltic Sea floor.

impact electricity availability and continuity in Estonia due to the limited number of critical power connections; for example, simultaneous failures of Estlink 1, Estlink 2, and the Latvia-bound connection would have significant consequences. While Estonia's installed net electricity generation capacity (2337 MW) exceeds peak consumption (1591 MW), the actual usable net capacity is lower due to outages, maintenance, and the availability of wind, solar, and hydropower resources (Elering, 2024c). The production capacity of oil shale power plants is approximately 1300 MW (ENTSO-E, 2024), including 274 MW from the Auvere power plant (Tooming, 2023).

From an environmental security perspective, Estonia does not have energy facilities that would cause severe environmental damage in the event of an accident. The primary external risk stems from potential incidents at nuclear power plants in neighboring countries, depending on wind direction. Such facilities include the Sosnovy Bor nuclear power plant in Russia and the Baltiysk and Astravets nuclear plants, as well as Finland's Olkiluoto and Loviisa plants, and potentially Hanhikivi in the future, along with Sweden's Oskarshamn nuclear plant. Estonia also lacks large hydroelectric power plants whose dam failure—either due to sabotage or structural collapse—could trigger a large-scale environmental disaster, such as the destruction of the Kakhovka hydroelectric dam in Ukraine in 2023.

The primary environmental hazards in Estonia relate to air pollution, fire, and explosion risks associated with dangerous enterprises. These risks are monitored, mitigation measures are in place, and drills are conducted (e.g., CREMEX in 2011 and CREVEX in 2023). Nevertheless, these remain the most probable risk scenarios. In the event of energy infrastructure failures, explosions at energy facilities would primarily have localized impacts, although the destruction radius and release of pollutants into the air could extend beyond the site, affecting nearby residential areas and ecosystems. The main environmental threat related to energy infrastructure failures in Estonia is air pollution. The highest technological and human-induced risks are associated with power plants and cogeneration plants. In the Tallinn area, for example, the Iru power plant operates as a combined heat and power facility, primarily using mixed waste and natural gas, with heavy fuel oil as a backup fuel (Enefit Green, 2021, p. 3). Under the Chemicals Act, Iru is classified as a Category B enterprise with a major accident hazard (Enefit Green, 2022, p. 3). Additionally, the OÜ Utilitas Tallinn power plant blocks are within a three-kilometer radius. The Iru plant processes approximately 250,000 metric tons of mixed waste annually (Enefit Taastuvenergia OÜ & Nomine Consult OÜ, 2017, p. 3).

Deliberate or accidental human-induced damage to energy and data connections and its possible consequences clearly pose the most significant risks to Estonia and the other Baltic states. Given the tense geopolitical situation in the region, various forms of hybrid attacks on electricity and gas infrastructure, as well as attacks on data cables, including cyberattacks and sabotage, are possible (Elering, Estonian Gas Transmission Network Development Plan 2024–2033, p. 8). A particular vulnerability lies in the high degree of integration between the Baltic states' electricity, gas, and data systems. Any disruption in electricity, gas, or data systems in one country inevitably affects the supply security in the other two. Minor disruptions are mainly reflected in fluctuations in service prices, while major outages that occur simultaneously across multiple sectors could lead to a reduction in the availability of critical services.

In addition to threats to subsea connections posed by human activity such as trawling and anchoring, the risk of deliberate sabotage amid escalating political tensions is becoming acute. Damage caused by human factors to various components of critical infrastructure

in the Baltic Sea region has increased, and there is mounting evidence linking these incidents to Russia's expansion of its subsea operational capabilities. The primary threat to the Baltic states arises from Russia, which possesses sufficient intelligence and resources to simultaneously target multiple subsea electricity, gas, and data connections in the Baltic Sea, potentially causing extensive network and service disruptions.

Following the escalation of the Russia–Ukraine conflict in 2022, the increasing number of deliberate sabotage incidents targeting subsea communication cables has raised concerns in many countries. In the case of Estonia and the other Baltic states, the risks are not limited to disruptions in subsea data connections but also include the electricity and gas pipelines running along the Baltic Sea floor. While disconnecting from Russia's energy system enhances the Baltic states' energy security, their dependence on subsea electricity and gas pipelines also introduces new security risks. A particular vulnerability lies in the possible simultaneous failure of multiple connections in the Baltic region (Trakimavičius, 2021).

Estonia's economy is highly dependent on the functioning of subsea gas pipelines, electricity cables, and communication cables in the Baltic Sea. The disruption of these connections poses significant risks to the continuity of critical services, affecting individuals, households, and, in the case of major failures, the broader functioning of society. Electricity consumption in Estonia, Latvia, and Lithuania exceeds domestic production by approximately 40% (Koppel, 2024). A shortage of electricity resulting from the failure of cross-border electricity connections could disrupt daily life and economic activities. While Estonia has sought to increase its controllable electricity generation capacity by opening the Auvere power plant and potentially reactivating the energy blocks at the Eesti and Balti power plants, these measures would be insufficient in the event of large-scale power outages (BNS, 2021). Estonia's normal electricity consumption far exceeds the production capacity of Auvere (Tooming, 2023), and restarting the energy blocks at the Balti power plant would be time-consuming, given their current state of preservation (ERR, 2024c).

As of the end of 2024, no decision had yet been made to develop additional controllable capacity (Koppel, 2024). In 2025, the Estonian government allocated funding to Eesti Energia for the construction of a gas power plant in Narva (Einmaa, 2025). However, this decision overlooks a key security consideration: constructing multiple such facilities near the border of an aggressive neighboring state is not advisable, as it reduces supply security in times of crisis. Estonia's gas consumption is also highly dependent on supplies from neighboring countries, meaning that disruptions in gas connections could directly impact household heating and industrial production processes. Furthermore, critical services such as healthcare, emergency services, transport, and food production rely heavily on energy and a stable international communications infrastructure. Any failure of subsea gas pipelines, electricity connections, or communication cables in the Baltic Sea could severely affect the continuity of these services, making it essential to factor such risks into mitigation planning.

Subsea electricity and communication cables in the Baltic Sea are strategically important not only for Estonia but also for other coastal states in the region to ensure economic security and stability across the area. However, the degree of dependence on these connections varies by country, depending on individual countries' infrastructure and energy production models. Estlink 1 and Estlink 2, which link Estonia and Finland, are particularly crucial for Estonia. Finland generates most of the electricity it needs (approximately 80 GWh annually) itself, importing a portion from Sweden, a smaller share from Norway,

and—until 2022—from Russia. In recent years, Finland's import volumes have nearly equaled its exports (Energiateollisuus, [n.d.]).

The NordLink connection between Norway and Germany, launched in 2021, provides a bidirectional solution: when Germany has excess wind and solar energy, Norway can import it; when Germany produces less renewable energy, Norway can export its hydroelectric power (Statnett, [n.d.]). However, NordLink is not critically important for the operation of critical services in either country, as both nations can generate sufficient electricity domestically or secure additional supplies through land-based connections with neighboring countries. The SwePol Link between Sweden and Poland offers Poland additional capacity, but only to a limited extent—approximately 1.5% of Poland's electricity consumption. In 2024, Sweden exported approximately 250 GWh of electricity to Poland each month (Svenska Kraftnät, 2024), which is a relatively small amount compared to Poland's total annual electricity consumption of 155,000 GWh (Statistics Poland, 2024).

To mitigate the effects of prolonged power outages on the population, the Estonian Rescue Board has conducted awareness campaigns and funded crisis preparedness projects for local governments, housing associations, and community organizations. As a result, several local governments, as well as some community organizations and housing associations, now have generators. However, while using a generator within the premises of a private house is relatively straightforward, apartment buildings require specific conditions to be met for generator use. Among community organizations, approximately a quarter are prepared to enact crisis-related measures (Savimaa & Kont, 2023, pp. 97–98), while among residents in private homes, about 34% report being able to manage for seven days, compared to just 3% of residents in large apartment buildings (Päästeamet, 2023).

A 2024 crisis preparedness survey conducted in Harku Municipality found that a significant majority (86%) of respondents had considered the possibility of a serious emergency over the past two years. The most critical services for residents were electricity supply, mobile phone service, water supply and sewerage, access to emergency medical care, and the continued operation of rescue services (Savimaa, 2024a, p. 34). However, only 15% of respondents viewed power outages as a major issue, and 30% believed they could cope with a power outage for up to 24 hours (ibid., p. 24). A similar survey conducted a year earlier in the Muuga area found that 13% of respondents considered power outages a significant problem, with 25% believing they could manage for up to 24 hours and another 25% for up to 48 hours (Savimaa, 2024b, p. 21). This suggests that as people have considered the possibility of short-term power outages—such as those in recent years, primarily caused by storms—they do not rank them as critical as failures in water supply, sewerage services, and mobile communications that result from prolonged electricity shortages or occur independently.

A 2024 study by Indrek Paadik on public awareness and preparedness for long-term crises in the field of internal security found that nearly half (40%) of respondents had food and water supplies for five to seven days, while 25% had provisions for at least 14 days (Paadik, 2024, p. 66). The most immediate impact of a failure in the Baltic Sea subsea power cables would be an increase in electricity prices in Estonia, which could, in turn, affect the cost of numerous services and the overall business environment. The failure of the Estlink 2 transmission cable in January 2024, which was only repaired in September, significantly influenced electricity prices in Estonia. For example, in July 2024, it was estimated that the outage contributed to a price increase of up to 42 euros per megawatt-hour (Randveer, 2024).

Severe consequences could also arise for telecommunications networks and infrastructure. In the absence of electricity, communication failures may occur, as most communication devices require power to function. Alternative connection routes to other countries do exist, following different physical pathways, but central data exchange nodes and their security remain the key vulnerabilities. Data transmission via the Baltic Sea submarine cables is supported by multiple alternative connections, and network traffic is automatically rerouted in the event of disruptions. Therefore, a single cable failure does not result in noticeable service disruptions for end users, but repairing damaged cables incurs direct costs that must ultimately be borne by consumers.

Completely securing land-based and seabed connections around the clock would be costly and complex. Therefore, it is crucial that potential risks are thoroughly assessed at both regional and national levels, and that detailed contingency plans are in place for responding to threats if they do materialize.

Gas supply interruptions primarily affect industrial enterprises and residents of apartment buildings or private houses that rely on gas heating or gas stoves. Gas heating and gas cookers are mostly found in apartment buildings constructed between the 1950s and 1970s, as well as in newer residential areas near gas pipelines (e.g., Viimsi Municipality and the city of Tartu). However, industrial enterprises are gradually reducing their dependence on gas. For example, the Iru power plant has decided to decommission its energy block No 2, which uses a gas-fired steam boiler. The waste incineration block and water heating boilers, which use natural gas but have diesel fuel as a backup, will remain in operation for now (Keskkonnaamet, 2024).

EXISTING RISK-MANAGEMENT PLANS AND THE SUFFICIENCY OF MITIGATION MEASURES

The increasing number of disruptions to subsea connections in the Baltic Sea has heightened awareness that Estonia's energy and data connections to the outside world are highly vulnerable in the event of potential conflicts and geopolitical tensions. The extensive integration and interdependence of the Baltic states' electricity, gas, and telecommunications networks makes this sector especially critical for ensuring supply security. Securing land-based and seabed connections around the clock would be both costly and complex. Therefore, it is crucial that potential risks are thoroughly assessed at both regional and national levels, and that detailed contingency plans are in place for responding to threats if they do materialize.

Security of Supply Report on the Estonian Electricity System (Elering, 2023a) states that there is a plan in place for ensuring the country's electricity supply, along with a backup plan and contingency plan for the backup plan. However, the report also notes that, following the damage to Balticconnector on 8 October 2023, concerns have grown over whether Estonia's infrastructure connections to other countries are adequately protected. The same report (Elering, 2023a) also highlights that the relevant infrastructure is dispersed across a large area, both on land and at sea, thus making it unrealistic to protect it entirely. Moreover, simultaneous targeted attacks in multiple locations could inflict enough damage to significantly disrupt the overall functioning of the system. Another major risk is the interdependence with other networks, such as the gas and data communications networks, which the report fails to address.

In addition to civil incidents, more attention should be directed to sabotage and subversion, which have become increasingly likely in the context of hybrid warfare.

Although risk assessments and contingency plans should, in theory, cover all potential threats and outline the necessary mitigation measures, there remains a possibility that not all events unfold as planned or that

new risks emerge that were not previously considered. According to Elering's risk manager (Soone, 2024), an updated electricity-and-gas-supply-continuity risk analysis and continuity plan is compiled every two years in accordance with the Emergency Act. To mitigate additional security risks, these documents are prepared for the Ministry of Climate, which oversees the continuity of critical services; these documents are not publicly available.

Publicly accessible contingency plans, however, only account for isolated individual disruptions, which are mitigated by ensuring sufficient reserve capacity. Elering maintains that the role of the system operator is to ensure the overall functioning of the system; the separate protection of individual connections has not been their priority so far. Yet, considering the recent case where two of Estonia's critical connections with Finland (Estlink 2 and Balticconnector) failed simultaneously—and given that the average time for repairing such failures is approximately six months—the risk to the continuity of critical services can be considered high, even with double redundancy connections in place. Nonetheless, Elering asserts (Soone, 2024) that such scenarios have been accounted for in risk assessments.

The Estonian Government Office notes that, in addition to civil incidents, there is a growing need to focus on sabotage and subversion—more likely in hybrid warfare—which necessitates additional protective measures.

The Estonian Government Office, responsible for developing Estonia's national crisis preparedness framework and legal regulations, as well as for improving resilience and overseeing crisis preparedness, has compiled a national risk analysis. This is the first comprehensive overview of various security threats and the potential impacts of major crises. This represents the first comprehensive overview of various security threats and the potential impacts of major crises, serving as the foundation for a broader risk analysis. According to the Government Office (Saar, 2024), existing risk analyses and risk-management plans for critical services do not fully address emerging security threats that have arisen since the start of Russia's war against Ukraine. Priit Saar, Deputy Director for National Security and Defense Coordination at the Government Office, notes that, in addition to civil incidents, there is a growing need to focus on sabotage and subversion—now more likely in hybrid warfare—which necessitates additional protective measures (Saar, 2024). The Government Office also considers sabotage and diversionary acts against Estonia's critical undersea infrastructure increasingly probable, calling for heightened security measures.

Before the disruptions to Balticconnector and Estlink 2, the Estonian Ministry of Economic Affairs and Communications maintained that these connections had already been secured during construction (Pulk, 2022). For example, Balticconnector is a thick metal pipe encased in an exceptionally durable concrete layer, and other cables have metal reinforcement. It was also pointed out that Estlink 1 and 2 quickly descend into deep waters from the mainland, a feature considered a natural protective barrier. However, the incident demonstrated that even a standard ship anchor can sever such connections in a brief period, potentially damaging multiple links simultaneously. According to Elisa Eesti AS's Chief Legal Officer, Allan Aedmaa (Aedmaa, 2024), it is not unlikely that a deliberate act could sever all of Estonia's underwater data connections to other countries at once.

Publicly available risk assessments by various organizations differ in their views on the importance and dependencies of these connections. For instance, Elering explicitly states in the *Estonian Gas Transmission Network Development Plan 2023–2032* that the Balticconnector project is critical for Estonia's supply security. Without it, a major system failure could necessitate restrictions on non-protected consumers—a risk eliminated by Balticconnector's completion. Meanwhile, the Estonian Min-

Russia has long manipulated energy supplies for political provocations.

istry of Economic Affairs and Communications asserts that damage to Balticconnector would not significantly affect Estonia (Põlluste, 2022) and has assured that spare parts for both Estlink connections are available and can be quickly used for repairs if needed. While disruptions could result in brief power outages of a few hours for lower-priority electricity consumers, the continuity of critical services would likely remain intact.

Elering's electricity supply security plan indicates that, drawing on tactics proven effective in Ukraine, Estonia is increasingly prepared to quickly resolve both intentional and accidental disruptions. According to Elering (Soone, 2024), since Russia's invasion of Ukraine, physical security risks to infrastructure have been thoroughly reassessed, and reserve stocks as well as new types of backup solutions have been significantly expanded to enable faster restoration of damaged infrastructure. However, the timeline for addressing the failure on 21 January 2024 shows that, despite these preparations, repairs could still take more than seven months. Given the potential for additional disruptions during this period, concerns about losing gas, electricity, or data connections are well founded.

Russia has long manipulated energy supplies for political provocations, and in the Baltic context, Moscow's actions are strategically aimed at targeting NATO member states' infrastructure in ways that demand a Western response. Within this framework, the Baltic Sea region—particularly the Baltic states—is seen less as a direct military target and more as a pressure point to weaken NATO, the United States, and the European Union (Galeotti, 2019; Kofman et al., 2021, p. 68; U.S. Army Asymmetric Warfare Group, 2015; Radin, 2017). Another risk to electricity supply security is that, after joining the continental European frequency area, the Baltic states remain connected to mainland Europe by only a single land-based transmission line. Currently, this connection is secured by the LitPol Link, established in 2015 between Lithuania and Poland. An additional connection was initially planned as a submarine cable for completion by 2026, but this project was abandoned due to rising investment costs and the growing number of underwater attacks. As a result, LitPol Link is expected to remain the sole electricity link between the Baltic states and continental Europe until about 2032, when a second land connection—planned to replace the canceled HarmonyLink submarine cable—will be completed.

Estonia also faces other risks to the continuity of critical services. Elering's 2022 security of supply report highlights the significant risk posed by gas supply disruptions. The Baltic states' gas systems are highly interconnected and influence each other substantially (Elering, 2023b, p. 22). During winter, when gas consumption is higher, greater inflows of gas are needed to maintain system pressure.

Gas consumption further increases when gas-fired power plants must produce more electricity—whether due to low renewable energy output or frequent power plant failures (Elering, 2023c, p. 8). Meanwhile, virtually all gas network equipment relies on electricity. Although power outages typically do not disrupt gas supply, they can hinder pipeline valve station controls. Notably, the Puiatu and Paldiski compressor stations require more electricity than backup generators can provide (ibid.), making it impossible to fully mitigate gas supply disruptions caused by power outages. These stations are critical for maintaining adequate pressure between Estonia and Finland.

From a security standpoint, the state also needs sufficient on-site fuel reserves for generators during power outages. Historically, the Estonian Stockpiling Agency focused primarily on liquid fuel reserves (Estonian Stockpiling Agency, 2024), keeping strategic quantities abroad for transport in emergencies. However, recent events in Ukraine have demonstrated potential pitfalls in relying on external reserves. Consequently, the agency plans to relocate its liquid fuel reserves to Estonia, exploring options including decen-

tralized storage with various service providers or using Milstrand's underground facility in Viimsi. The latter would require additional measures to ensure reserve access during prolonged power outages (ERR, 2022).

Turning to data transmission, Gehringer (2023, p. 3) argues that a complete shutdown of data traffic is currently unlikely. Damage to a single cable does not cause a total loss of transmission if alternative internal network routes are available. If certain cable connections fail, data can be rerouted, though this may lead to higher latency and network congestion. Gehringer (ibid.) notes that a simultaneous physical attack on multiple submarine cables, while possible in theory, would require extensive knowledge, resources, and preparation. The public availability of cable routes and landing points adds to security concerns, making it critical to incorporate such threats into various scenarios. Wall and Morcos (2021) likewise emphasize that scenario-based planning helps governments and infrastructure owners identify key national contacts, conduct regular drills, and enhance system resilience. They suggest that such planning should be a priority for EU–NATO cooperation, leveraging the EU's financial and regulatory tools alongside NATO's defense planning expertise.

If Estonia's submarine data connections were disrupted, land-based connections via Latvia would serve as the fallback. However, these alone cannot guarantee the necessary quality of data transmission. Theoretically, such an approach could support critical services, but a prolonged outage would require restrictions on consumer internet use. In practice, relying solely on land connections for critical services has yet to be fully assessed. To strengthen the continuity of critical services, the State Infocommunication Foundation (RIKS) is developing a national satellite communication project (Pau, 2023).

A detailed assessment of the adequacy of existing risk-management plans and mitigation measures has become increasingly complex due to the rapid shifts in the security landscape in recent years, as well as the evolving nature and variability of associated risks. This situation has also been influenced by broader crises not directly related to hybrid attacks on underwater infrastructure in the Baltic Sea, such as the COVID-19 pandemic, which exposed vulnerabilities in supply chains. According to Glette-Iversen, Flage, and Aven (2023, p. 11), this underlines the need to update risk assessment methodologies. In the absence of robust risk analysis, unexpected incidents can arise for five key reasons: inadequate probability assessment, insufficient modeling of cause-and-effect relationships, weak early warning systems, limited capacity to reduce uncertainty, and a lack of knowledge and understanding. This, in turn, constrains precautionary capacity (Glette-Iversen & Flage, 2024, p. 2).

The impact of infrastructure failures has typically been assessed separately from two perspectives: that of service providers and that of national integrated operation. However, Hansen and Antonsen (2024, p. 2) argue that security considerations should also be incorporated into risk and safety assessments at both the organizational and technical levels, despite the frequent absence of a unified conceptual understanding of risk in both theoretical and applied contexts (Aven, 2023, pp. 3–5). As a result, safety and human factors should be integrated into a comprehensive safety and security analysis. However, excessive generalization of details complicates such analysis, diminishing its practical value and leaving considerable uncertainty in system assessments (Nolan-McSweeney, Ryan & Cobb, 2023, p. 13). Eriksson (2023) suggests that risk analysis and crisis prevention should become an integral part of an organization's continuous learning system. Nevertheless, in Sweden, these approaches are currently underused in the contexts of prevention and preparedness at local, regional, and national levels (Eriksson, 2023, pp. 5–6).

The existence of these issues is further confirmed by an Estonian National Audit Office review, which found that physical security requirements have been defined (and met) at only one electricity supply facility in Estonia—also the only one officially designated as a national defense site. Other critical electricity supply buildings and infrastructure have not been classified as national defense sites, meaning that the choice of physical security measures is left to the discretion of the companies operating them. In many cases, these measures are weaker than those implemented at designated national defense sites. (Riigikontroll, 2025, pp. 1–9)

If Estonia's submarine data connections were disrupted, land-based connections via Latvia would serve as the fallback. However, these alone cannot guarantee the necessary quality of data transmission.

MONITORING AND PROTECTION OF CRITICAL UNDERSEA INFRASTRUCTURE IN THE BALTIC SEA

Critical infrastructure covers networks, services, resources, and institutions essential for the functioning of a state, where any disruption can significantly impair national operations (Sõmer et al., 2019). Although its protection represents a strategic priority, in practice, the oversight and responsibility for subsea infrastructure remain unclear. At the European Union level, this issue has gained prominence in recent years, with increasing calls for member states to clarify national-level authorities responsible for the security and protection of submarine cables (European Commission, 2024b; Bafoutsou et al., 2023, p. 24).

The greatest challenge with subsea connections is that they extend into international waters, making it difficult to establish clear jurisdiction over their oversight and control. While these connections are subject to various national and international laws and agreements, practical enforcement remains complicated due to the overlapping rights and responsibilities of various stakeholders, such as telecommunications and energy companies, cybersecurity agencies, military forces, and coast guards. Bueger et al. highlight in their 2022 report for the European Parliament's Subcommittee on Security and Defense (Bueger et al., 2022, p. 41) that although EU agencies such as the European Border and Coast Guard Agency (Frontex), the European Defense Agency (EDA), the European Environment Agency (EEA), the European Fisheries Control Agency (EFCA), the European Maritime Safety Agency (EMSA), and the European Union Agency for Cybersecurity (ENISA) all have relevant mandates concerning subsea infrastructure, none is explicitly tasked with the protection and resilience of data transmission cables.

ENISA conducted a comprehensive review of the subsea connection system in 2023 (Bafoutsou et al., 2023) and provided recommendations for both infrastructure owners and national governments. They noted that in coastal and territorial waters (up to 12 nautical miles) and exclusive economic zones (up to 200 nautical miles), submarine cables are protected by the Navy, military, and national coast guards. However, in international waters, particularly beyond exclusive economic zones, authority is more ambiguous, and it is not explicitly defined which state is responsible for monitoring and protecting submarine cables.

The Nord Stream gas pipeline explosions highlighted the practical challenge that, for the affected state bearing the burden of proof, it is difficult to hold another state accountable for an act of sabotage in the maritime environment, as it allows for the concealment of evidence regarding the attack's origin (Lott, 2023a). When an attack occurs in territorial waters, the legal framework grants the victim state greater freedom to respond, as a coastal

The greatest challenge with subsea connections is that they extend into international waters, making it difficult to establish clear jurisdiction over their oversight and control. Finland's decisive response has set a highly significant precedent in this regard.

state's sovereignty extends to its territorial waters in addition to its land territory. Therefore, if a state employs armed force against critical maritime infrastructure in another coastal state's territorial waters, this could serve as grounds for invoking the right to armed self-defense, as territorial waters are considered sovereign territory. However, if an attack takes place in the exclusive economic zone, the right to armed self-defense applies only if the attack has a significant impact on the coastal state and the state can meet the burden of proof (ibid.).

In the case of Nord Stream, no evidence could be established to prove that another state was behind the attack. Furthermore, an additional factor in the Nord Stream incident was the lack of a clear link to the specific coastal state, meaning there was no legal basis to classify the sabotage as an attack against the state whose exclusive economic zone it occurred in. Even in cases where sabotage is confirmed and legally recognized as an armed attack against a coastal state, an additional requirement is that the incident must have a significant impact on the continuity of critical services in that state. Yet even then, the perpetrator must be identified and proven responsible. It is crucial to prevent future scenarios where the destruction of infrastructure located in an exclusive economic zone, but not directly linked to the shore, remains unanswered by the affected state. Sweden's decision not to assign clear responsibility for the Nord Stream attack is a clear example of why the attack was carried out specifically within its exclusive economic zone—this must be interpreted as an attack against the state's security-related legal order.

According to the 1982 United Nations Convention on the Law of the Sea (UNCLOS), coastal states have the right to adopt regulatory legal acts concerning, among other things, the protection of cables and pipelines (UNCLOS, Art. 21, para. 1). Article 113 of the convention requires states to adopt laws and regulations making it a punishable offense for a ship flying its flag or a person under its jurisdiction to willfully or through culpable negligence break or damage a submarine cable beneath the high seas, if such an act interrupts or obstructs telegraphic or telephonic communications. The provision equally applies to the breaking or damaging of a submarine pipeline or high-voltage power cable. It also covers conduct likely to result in such breaking or damage. Therefore, for each case, a direct link between a specific state and a vessel flying its flag must be clearly established in connection with a deliberate act of sabotage, with the expectation that the relevant state will enforce the applicable legal measures. However, in practice, this approach is insufficient. Recent incidents have highlighted the clear need for European coastal states to introduce additional restrictions under Articles 60(4)–(6) of UNCLOS in areas surrounding critical infrastructure in their exclusive economic zones and to implement stricter enforcement measures in response to violations in these zones (Lott, 2023a).

On 26 February 2024, the European Commission adopted Recommendation 2024/779 on secure and resilient submarine cable infrastructures. Among other points, the recommendation calls for the establishment of an expert group composed of representatives of member state authorities to facilitate information exchange and cooperation between member states and the Commission. The group aims to identify gaps in the current legal framework and enhance synergies in addressing them. Additionally, it seeks to share information on situational awareness, incidents and responses, and best practices.

In Estonia, no regulation explicitly defines which authority is responsible for the security and monitoring of subsea connections essential to the continuity of critical services. Chapter 5 of the Emergency Act lists critical services alongside the authorities responsible for their continuity. Under this framework, the Ministry of Economic Affairs and

THE SECURITY AND MONITORING OF UNDERSEA CONNECTIONS TO PREVENT DELIBERATE DAMAGE IS A COMPLEX CHALLENGE. PHOTOGRAPH: PEXELS.COM

Communications oversees the continuity of data transmission services, while the Ministry of Climate is responsible for electricity and gas supply continuity. According to Section 15 (4) of the Emergency Act, the authority responsible for the continuity of a critical service must develop an emergency response plan for managing emergencies caused by an interruption with severe consequences or prolonged disruptions. Section 38 of the Act establishes the obligations of critical service providers, requiring them to conduct continuity risk assessments, develop continuity plans, implement preventive measures against disruptions, and ensure the quick recovery of services in the event of an emergency, technical failure, or the interruption of another critical service.

In addition to these provisions, the Emergency Act specifies the requirements for ensuring the continuity of each critical service. For example, natural gas suppliers must secure additional gas supplies, electricity companies must maintain backup power reserves to balance Estonia's electricity system, and telecommunications providers must ensure autonomous power supply for their networks. However, no existing legislation explicitly requires critical service providers to conduct independent monitoring and oversight of their own infrastructure, including subsea connections. This is confirmed by Elering's risk manager, Peep Soone (2024). At the same time, the Minister of Defense has stated that the responsibility for continuous infrastructure monitoring lies with the infrastructure operator—in this case, Elering (Lauri, 2023).

The Estonian Navy is responsible for maritime surveillance in Estonia's maritime area, but the current legal framework does not provide specific guidelines or designate a primary authority for the protection and security of subsea infrastructure.

In Estonia, surface surveillance is carried out by the Estonian Navy's Maritime Operations Center, which is responsible for monitoring surface activities up to the outer boundary of

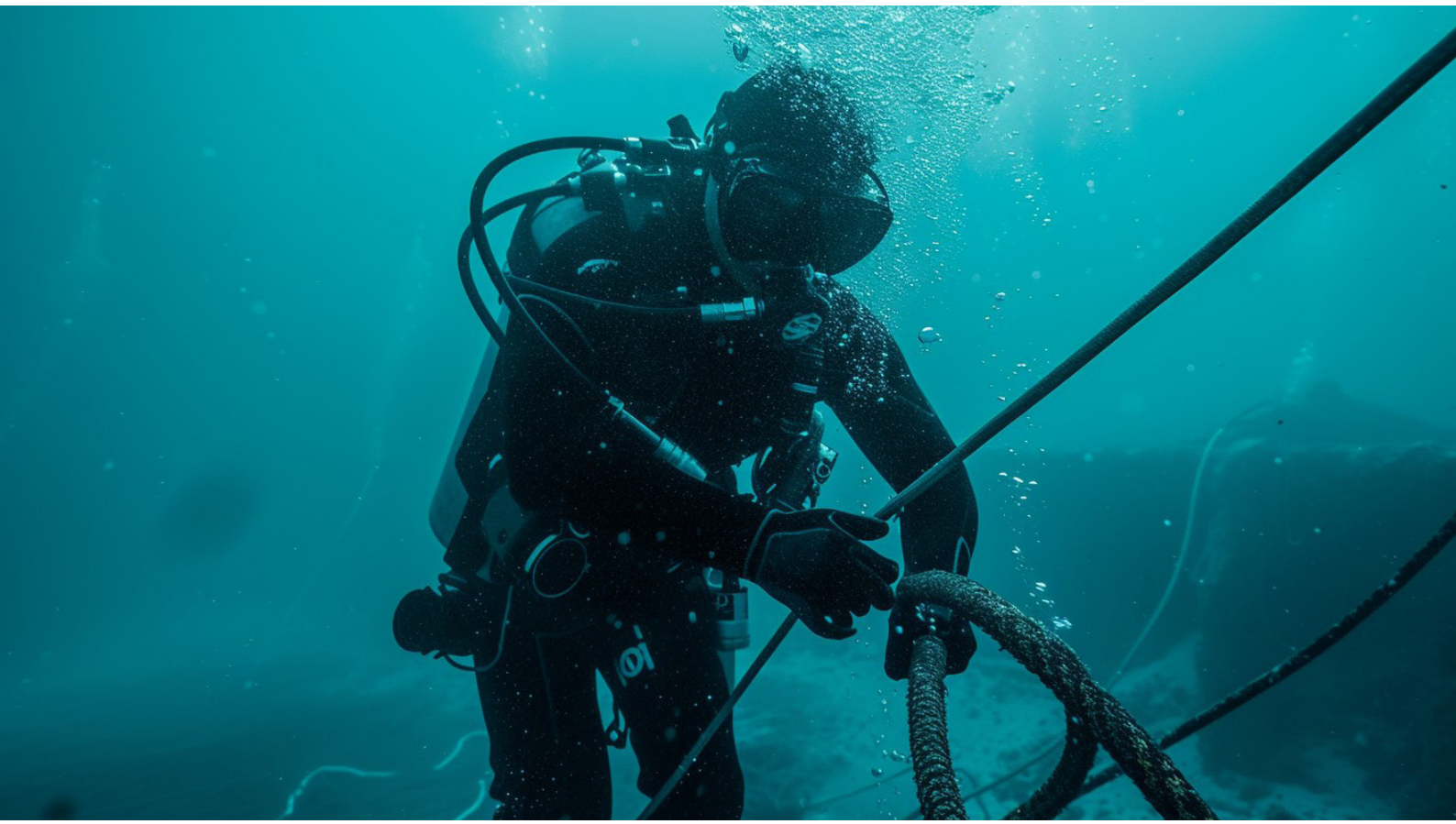
Estonia's exclusive economic zone. These responsibilities derive from the Defense Forces Organization Act, the Defense Forces Statute, and the Navy Statute. However, the Estonian Navy does not have a specific mandate for monitoring submarine electricity, gas, or data transmission connections, although it endeavors to perform this function within its operational capacity. According to the head of the Navy's Maritime Operations Center, Ardo Riibon (2024), surveillance is conducted by the Center's operators who monitor surface traffic, particularly in the vicinity of critical infrastructure. He adds that the Navy is legally obliged to ensure maritime surveillance in Estonia's maritime area, but the existing legislation on subsea infrastructure security does not provide clear guidelines or designate a primary responsible authority. Moreover, the Navy has not previously received specific instructions on how to carry out these tasks. Nonetheless, the Navy has taken it upon itself to conduct monitoring in the immediate vicinity of subsea infrastructure among other operations.

According to Riibon (2024), attention is focused primarily on the Estlink 1 and Estlink 2 connections, and operations are guided by the European Union's maritime security strategy and its action plan, as well as the recommendations of NATO's Critical Undersea Infrastructure Network working group, which operates under NATO's Maritime Command (MARCOM). The security and integrity of subsea infrastructure undoubtedly pose a challenge, particularly when responsibility ends where a cable or pipeline exits a state's exclusive economic zone, leaving open the possibility of deliberate damage. This issue is especially relevant for Estonia in the Gulf of Finland, where critical connections between two NATO countries pass beneath the main waterway linking Russia to the Baltic Sea.

A further challenge concerns how to respond to a threat or hostile actor detected near critical maritime infrastructure. Section 47 of the Defense Forces Organization Act specifies the rights and responsibilities for countering threats posed by civilian aircraft, but the law does not address threats from vessels at sea. The Government Office (Saar, 2024) has also highlighted the need to strengthen response measures for incidents like those caused by the *Newnew Polar Bear* in October 2023.

The principle guiding threat mitigation must be that the destruction of state-owned or critical service infrastructure is illegal and must be prevented under all circumstances. Although the Navy does not yet have a clearly defined legal mandate regarding subsea infrastructure, it is currently the only authority in Estonia with the necessary capabilities in this area. The role of the Defense Forces is to ensure Estonia's military defense, which has broader implications for society, including responsibilities arising from the comprehensive national defense concept. Furthermore, the responsibilities of the Navy have expanded significantly following the integration of the Police and Border Guard Board's fleet into its command structure. The Navy can also provide operational support to other state authorities using the resources at its disposal. Thus, under the principle of subsidiarity in public administration, expectations regarding responses in areas not explicitly defined by law should be assigned to the state authority that is both regulatively and functionally closest to the task, with the right to request the necessary professional assistance for national defense purposes.

Maritime surveillance has become increasingly important due to the interest that the Russian Navy has recently shown in underwater infrastructure in the Baltic Sea, as identified by Nordic intelligence services (Lauri, 2023). The Estonian Navy has previously raised concerns about the activities of the Russian Navy and intelligence services (Sprenger, 2019). However, even when specific violations are detected, the legal options for intervention remain limited. Under Article 110 of UNCLOS, a warship on the high seas is permitted to board a foreign vessel only if there is reasonable suspicion that the



RUSSIA'S INTEREST IN AND CAPABILITY FOR SABOTAGING UNDERSEA CONNECTIONS HAVE RECENTLY INCREASED. PHOTOGRAPH: STOCKCAKE.COM

vessel is engaged in piracy, involved in the slave trade, conducting unauthorized broadcasting, without nationality, or flying a foreign flag or refusing to show its flag while in reality belonging to the same nationality as the warship. A coastal state has the right to pursue a foreign vessel only if it is suspected of having violated the laws of the state's internal waters, archipelagic waters, territorial waters, or contiguous zone. This right of pursuit ceases as soon as the pursued vessel enters the territorial waters of its own or a third country.

According to the head of the Estonian Navy's Maritime Operations Center (Riibon, 2024), considerable progress has been made over the past year in improving inter-agency communication and operational protocols, as well as in planning investments to enhance surveillance. The locations, specifications, and installation details of various connections have been mapped in greater detail to enable faster responses to potential incidents. At the national level, the goal is to increase the surveillance and protection of critical undersea infrastructure in the Baltic Sea and to support the development of a pan-European monitoring system to ensure cross-border service continuity (Eesti Euroopa Liidu poliitika prioriteedid 2023–2025, p. 7).

The Estonian Navy has increased patrols and monitoring near the Estlink 1 cable and other critical underwater infrastructure (Kilumets & Teppan, 2024). The Defense Forces have previously carried out exercises to protect critical undersea infrastructure, for example, during the Joint Expeditionary Force's Nordic Warden series of protective military activities in June 2024 (Kaitsevägi, 2024). The Estonian Parliament's National Defense

Committee has stated that appropriate steps must be taken to protect underwater infrastructure, including the establishment of a permanent naval presence in the Baltic Sea, like NATO's Baltic Air Policing mission, with one of its tasks being the protection of subsea infrastructure (Postimees, 2024b). Following the seizure of the *Eagle S* by Finnish authorities, the Estonian government has also increased the monitoring and protection of critical infrastructure in the Baltic Sea (Vabariigi Valitsus, 2024; ERR, 2024d), involving allied partners.

4. CHALLENGES AND DEVELOPMENT NEEDS

Experts consider continuous monitoring and security of all underwater energy and data connections unfeasible. Preventing and detecting underwater attacks requires specialist surveillance technology along the entire length of these connections, which in turn increases the likelihood of targeted attacks, as many states are reluctant to disclose information about their submarines' movements. For Estonia, it is essential to develop clear guidelines for preventing potential threats and responding swiftly if they materialize. Additionally, well-structured agreements and contingency plans must be in place to address scenarios that could disrupt the availability of the country's critical services.

CONSTANT MONITORING OF ALL UNDERSEA CONNECTIONS IS UNFEASIBLE. PHOTOGRAPH: STOCKCAKE.COM

EUROPEAN UNION AND NATO COOPERATION IN PROTECTING CRITICAL UNDERSEA INFRASTRUCTURE

Both international organizations and relevant national authorities, as well as infrastructure operators, emphasize that improving cooperation and information exchange between stakeholders is essential for better risk management. The report "Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU" (Bueger et al., 2022, p. 52) highlights a series of recommendations to enhance the protection of subsea infrastructure at the EU level. One of the most critical actions identified is raising awareness among institutions within member states and incorporating cable protection needs into the planning of new strategic initiatives. Following the acts of sabotage in the Baltic Sea, the European Commission further expressed its desire for EU member states to enhance cooperation in protecting cables and other underwater infrastructure (European Commission, 2024b; Pollet, 2024). Various discussions and consultations are currently taking place at the European Union level with member states, civil society, industry, and academia to shape the background for future proposals by the European Commission. However, a key shortcoming of this framework is its predominant focus on data and digital infrastructure.

Particular attention must be given to potential threat scenarios whereby multiple cables and energy connections are severed within a short period. Well-developed contingency plans must be in place for such incidents.

Given the war in Ukraine and NATO's expansion, transatlantic allies must work together to strengthen the protection of their underwater infrastructure against Russia's hybrid tactics (Nakamura, 2023; Loik, 2024). Several analyses had already highlighted the vulnerability of submarine critical infrastructure and the need for closer cooperation between NATO and EU countries before the Ukraine conflict escalated into full-scale war. These analyses also provided concrete recommendations for such collaboration. For example, Wall and Morcos (2021) advised that the United States, with its European allies and partners, should work closely with the private sector to develop plans for handling the consequences of deliberate (or accidental) subsea infrastructure disruptions. Special focus should be placed on scenarios where multiple cables are cut within a short period or simultaneously.

The European Union and NATO intensified their cooperation on critical infrastructure protection following Russia's full-scale aggression against Ukraine on 24 February 2022. This cooperation gained urgency after the sabotage of the Nord Stream gas pipelines on 26 September 2022 and the destruction of the Balticconnector pipeline between Finland and Estonia on 8 October 2023. During the latter incident, Estonia–Finland and Estonia–Sweden subsea communication cables were also damaged. In response, NATO increased air and naval patrols and its presence in the Baltic and North Seas under the UK-led Joint Expeditionary Force (JEF) (NATO, 2023c). However, these measures did not sufficiently deter Russia, as subsequent attacks on Baltic Sea infrastructure using Russia's shadow fleet demonstrated.

At the Vilnius Summit in July 2023, NATO member states agreed to establish a Maritime Center for the Security of Critical Undersea Infrastructure under NATO's Maritime Command (MARCOM) in the United Kingdom. Additionally, a dedicated cooperation network was created to connect NATO member governments with the private sector and other relevant stakeholders to improve information exchange and develop best practices (Vilnius Summit Communiqué, 2023, point 65; Monaghan et al., 2023, p. 1). It is also worth noting NATO's maritime security operation Sea Guardian, which, among other

tasks, focuses on enhancing situational awareness, counterterrorism, and response capability development in the Mediterranean region.

As member states strive to integrate innovative technologies into their navies, NATO's Science and Technology Organization (STO), based in La Spezia, Italy, is expected to play an increasingly significant role in providing innovative, science- and technology-based solutions to close maritime capability gaps (Fridbertsson, 2023, pp. 8–9). For example, NATO is accelerating the development of technologies that allow for real-time detection of suspicious activity near critical undersea infrastructure. These include testing maritime drones and various sensor systems and the application of artificial intelligence. In future developments, smart fiber-optic cables may detect activity occurring nearby (Lima & Drozdiak, 2023). While next-generation surveillance solutions are still under development, joint capabilities must already be implemented today.

Cooperation to strengthen critical infrastructure became even more crucial following the sabotage of the Nord Stream pipelines and in response to Russia's weaponization of energy as part of its war of aggression against Ukraine. In February 2023, NATO launched a Critical Undersea Infrastructure Coordination Cell at its headquarters. Earlier the same year, NATO and the European Union jointly established a Task Force on Resilience of Critical Infrastructure, which focuses on energy, transport, digital infrastructure, and space sectors (NATO, 2023a; 2023b). These cooperation frameworks are recent and require time to become fully operational, but they are undoubtedly necessary steps for resource planning and consolidated capability development. This is particularly crucial for smaller member states that lack the individual expertise and resources for integrated defense solutions, which require surface, underwater, and aerial components.

Close cooperation between the European Union and NATO in protecting critical undersea infrastructure is particularly essential for smaller member states, which lack the expertise and resources for integrated defense solutions on their own.

One of the most significant recent developments in the European Union regarding the protection of critical undersea infrastructure has been the revision of the EU's maritime security strategy and its action plan in 2023 (European Union, 2023). This update introduces a range of measures to enhance the resilience and protection of critical maritime infrastructure, including gas pipelines, electricity and data cables, ports, offshore energy facilities, LNG terminals, and floating storage and regasification units. The EU strategy and action plan also outline steps to improve cybersecurity, counter information manipulation, and strengthen resilience against hybrid threats related to maritime security. Estonia, in cooperation with its Baltic Sea allies, should adopt an active stance in NATO and EU formats on the development of undersea infrastructure protection capabilities, given that Estonia is particularly vulnerable in this domain, and developing independent capabilities in this field is highly resource-intensive for any individual country.

On 21 February 2024, the European Commission introduced the white paper "How to master Europe's digital infrastructure needs?" (European Commission, 2024c), aimed at initiating discussions among stakeholders, member states, and like-minded partners to reach a consensus on future European policy concerning submarine cable infrastructure. The document also includes recommendations to enhance the protection and resilience of submarine cables by improving governance and financing coordination across the EU. These measures include assessing and mitigating security risks, developing a cable security measures package and simplifying permit procedures (European Commis-

Estonia, in cooperation with its Baltic Sea allies, should adopt an active stance in NATO and EU formats on the development of undersea infrastructure protection capabilities, given that Estonia is particularly vulnerable in this domain, and developing independent capabilities in this field is highly resource-intensive for any individual country.

sion, 2024). To support these recommendations, a public consultation was launched on 12 scenarios outlined in the white paper, alongside the formation of an expert group on submarine cable infrastructure comprising member state authorities (ibid.).

However, Hendriks and Halem (2024, p. 30) argue in their report that, despite suspicions of Russian involvement in cable disruptions in the Baltic Sea in October 2023, the EU's plan to increase investment in diversifying its cable network from 2024 remains insufficient. The preliminary proposal still relies on non-binding recommendations to member states rather than providing the necessary impetus to address this critical strategic challenge. The report is also critical of the fact that, while NATO and the EU have established commissions and new bodies dedicated to undersea protection, these efforts primarily focus on defining the situation and formulating strategic concepts rather than coordinating capability development and conducting regular joint operations to create an interconnected defense system against hostile activities (Hendriks & Halem, 2024, p. 11). Additionally, the EU currently lacks sufficient resources to fund projects for laying and protecting underwater cables (Pollet, 2024). The Commission document lists several potential sources of additional funding, including increased national contributions from member states and amendments to state aid rules (European Commission, 2024b).

At the Summit of Baltic Sea Allies in Helsinki on 14 January 2025, NATO Secretary-General Mark Rutte announced the launch of Operation Baltic Sentry to strengthen the protection of critical undersea infrastructure in the Baltic Sea. This surveillance mission includes frigates, maritime patrol aircraft, and naval drones, while also enhancing cooperation with allies to integrate surveillance systems and improve the protection of critical underwater infrastructure (NATO, 2025). The Allied Joint Force Command Brunssum (JFCBS) will oversee the operational command of Baltic Sentry, in coordination with NATO's Maritime Command (MARCOM) (SHAPE, 2025). In a joint statement (Tasavallan Presidentti, 2025), Baltic Sea NATO allies emphasized their determination to prevent, detect, and counter sabotage attempts and meet any attacks on their infrastructure with "a robust and determined response." The main protective measures highlighted include:

- Deploying innovative solutions and innovative technologies for the surveillance and tracking of suspicious vessels and undersea monitoring, including enhanced partnerships with the private sector, in particular infrastructure operators and innovative technology companies.
- Active information exchange and incident assessment to analyze trends and share best practices for response.
- Expanding NATO–EU cooperation, including in responding to the threats caused by the reckless activities of vessels serving Russian cargo flow.
- Under international law, acting against any suspected vessels that circumvent sanctions and threaten the security, infrastructure, and environment of NATO states.
- Increasing the surveillance of vessels through close coordination among coastal states, including more efficient inspections of vessel insurance certificates.
- Deploying additional tracking tools and expanding sanctions targeting the shadow fleet.

READINESS FOR FAULT RECTIFICATION AND ACCELERATING RESPONSE PROCESSES

Practical cases have shown that one of the most serious risks to ensuring the continuity of a state's critical services is the time required to repair damaged connections. The risk level increases further when prolonged repair periods lasting several months coincide with unplanned disruptions. Additional concerns arise from the fact that only a limited number of organizations in Europe specialize in repairing subsea infrastructure, making their availability highly constrained when multiple failures and unplanned outages occur simultaneously (Bueger et al., 2022, p. 28). Globally, there are approximately 60 vessels dedicated to laying and maintaining undersea cables, many of which are already committed to new cable-laying projects under long-term contracts (Swinhoe, 2022). Most of these vessels are privately owned, posing a potential security risk, as states engaged in espionage and sabotage may seek to exploit their activities for their own interests (Kuszynski & Barns, 2022, p. 11).

For both Estonia and other nations, it is crucial to ensure that the physical monitoring and restoration of critical subsea infrastructure are secured through appropriate contracts and the necessary stockpile of materials.

For both Estonia and other nations, it is crucial to ensure that the physical monitoring and restoration of critical subsea infrastructure are secured through appropriate contracts and the necessary stockpile of materials. The Ministry of Climate has directed Elering, as the system operator for electricity and gas connections, to sign an emergency repair readiness contract for electricity cables by 2024. According to the Estonian Navy (Riibon, 2024), its available resources are sufficient to monitor surface activity near critical underwater infrastructure and it also possesses the capability to inspect underwater assets if concerns arise. However, the technical equipment currently in use was not specifically designed for this purpose. Using tools originally intended for mine detection makes the inspection process slow and resource-intensive. Therefore, service providers must secure agreements with reliable partners capable of inspecting and repairing connections within a reasonable period. The Estonian Government Office also emphasizes (Saar, 2024) the critical importance of having such contracts to enable rapid response to failures. The primary reason for this is the limited number of specialists and companies in neighboring countries capable of repairing subsea connections. In the event of major incidents or attacks, several countries would be competing for the same resources.

FAULT RECTIFICATION OF SUBSEA INFRASTRUCTURE REQUIRES SPECIFIC EQUIPMENT AND TECHNOLOGY.
PHOTOGRAPH: STOCKCAKE.COM

REDUCING DEPENDENCE ON TECHNOLOGY PRODUCED IN CHINA

At the European Union level, concerns have been repeatedly raised about the People's Republic of China's efforts to gain control over Europe's strategic sectors through targeted investments. It has been emphasized that China has acquired critical infrastructure, particularly within the EU and its neighboring regions, including the Western Balkans and Africa, posing an increasingly multidimensional security threat to the EU (European Parliament, 2024). In its 2024 annual review, the Estonian Foreign Intelligence Service (Välisluureamet, 2024, p. 75) similarly warns that both the public and private sectors should proactively prevent the excessive spread of Chinese technology. The annual review highlights that this is a deliberate state-driven strategy by China, aimed at reaching a point where integrated technology solutions cannot be replaced with Western alternatives due to incompatibility and entanglement. However, it also notes that Chinese companies offer products and services at lower prices, which, under public procurement rules that favor the lowest bid, may require a reassessment of procurement policies in the public sector. Member states must be able, particularly for critical products and services, to ensure that third-country suppliers presenting security risks can be excluded (Eesti Euroopa Liidu poliitika prioriteedid 2023–2025, p. 7).

For Estonia, one key risk area lies in the planning of large-scale future investments in the energy sector. Cross-border network investments currently in development include the third Estonia–Finland connection, the fourth Estonia–Latvia connection, and the Baltic Sea Grid development project (Elering, 2023a, p. 58). Both Huawei and other Chinese companies have already expressed interest in supplying inverters and energy storage systems for Estonian solar and wind farms (Estonian Foreign Intelligence Service, 2024, p. 75). However, Elering's representative (Soone, 2024) states that current public procurement regulations do not allow for a complete exclusion of such suppliers. This is confirmed by Government Office representative Priit Saar (Saar, 2024), who adds that although a policy decision to avoid Chinese technology in public procurement was made in 2023, there is currently no legally watertight solution. The procurement system still allows participation from companies with indirect ties to China, enabling the continued distribution of Chinese-produced technology through intermediary firms.

LEGAL FRAMEWORK FOR PROTECTING UNDERSEA INFRASTRUCTURE

The biggest challenge in protecting undersea connections is establishing sufficient national and international regulations to prevent the recurrence of deliberate attacks against infrastructure on the high seas, as attributing responsibility for such incidents to specific actors remains overly complex. The recent high-profile cases include the Nord Stream pipeline explosions, which took place in the exclusive economic zones and continental shelves of Denmark and Sweden. These incidents were not legally classified as attacks on either coastal state, as they occurred in international waters and therefore did not trigger the right to armed self-defense (ERR, 2023c). Additionally, on 7 February 2024, the Swedish Prosecution Authority announced the closure of its investigation into the destruction of the Nord Stream 1 and 2 pipelines, handing over the collected evidence to Germany. It justified the decision by stating that Sweden lacked jurisdiction to continue the case since the preliminary investigation found no involvement of Swedish nationals in the alleged sabotage (Postimees, 2024a).

Amending UNCLOS would require consensus from all ratifying states.

These explosions have been described as acts of sabotage against pipelines and cables, which may constitute criminal offenses

under certain coastal state laws but are not explicitly prohibited under the current legal framework of the law of the sea (Azaria & Ulfstein, 2022). Both cybersecurity and maritime domains have increasingly become gray zones for warfare and hybrid threats (Bueger et al., 2022, p. 31). The United Nations Convention on the Law of the Sea (UNCLOS), established in 1982, and its supplementary legal acts are now outdated and inadequate considering recent incidents, allowing for continued impunity for hostile activities against undersea infrastructure. However, the main obstacle to updating UNCLOS is that all ratifying states would need to agree to the amendments, which is an unlikely scenario given diverging interests among stakeholders. Consequently, a fundamental principle must be upheld: attacks on property and assets are illegal regardless of whether they are specifically listed. It is highly improbable that a perpetrator who used explosives to destroy infrastructure would later challenge their prosecution in court, and the court would rule that such an attack was not prohibited under maritime law.

Estonia encountered comparable legal gaps following the October 2023 Balticconnector and data cable incidents. The 2024 annual report of the Estonian Internal Security Service (Kaitsepolitseiamet, 2024, p. 54) notes that the damage occurred in Estonia's exclusive economic zone but outside its territorial waters, leaving the authorities without a clear legal basis under international law to intercept the suspect vessel or investigate on board. Despite these limitations, both Estonia and Finland requested legal assistance from China to obtain vital information. According to maritime law expert Alexander Lott (Lott, 2023b), Estonia and Finland should consider establishing safety zones around undersea cables and pipelines in their exclusive economic zones, in line with UNCLOS Article 60(4–6), to improve protection. In 2023, Lott also suggested that if a foreign vessel were to damage undersea connections in Estonia's exclusive economic zone, Estonian authorities should set an international precedent by boarding and potentially detaining the vessel in the Baltic Sea, citing the need to protect the marine environment. Finland took a similar approach in December 2024 after a separate incident.

The Estonian Navy, responsible for overseeing Estonia's undersea infrastructure, emphasizes that coastal states must update their legislation to address emerging threats and risks. It notes that violations are often detected, yet the existing legal framework provides insufficient recourse. Regulatory changes are also needed to enable a shift from merely reacting to security incidents toward actively preventing them.

In the event of a kinetic conflict or preceding hostile posturing, there are several non-military steps that the collective defense alliance opposing Russia could take, particularly concerning Kaliningrad, to strengthen its position and protect undersea connections. The most formal step would be for Finland and Estonia to revoke their 1995 bilateral agreement on the width of territorial waters, which currently leaves a three-nautical-mile international shipping corridor on either side of the Gulf of Finland's median line. Terminating this agreement would make the Gulf of Finland de jure inaccessible to Russian vessels. Additionally, Denmark and Germany could impose restrictions on Russian maritime traffic through the Danish Straits and the Kiel Canal, limiting Russia's ability to transport LNG from its Western Siberian or Far Eastern production facilities into the Baltic Sea. The downside of this solution is that while ships are currently required to remain in international waters, in certain cases, when passing through the exclusive economic zone, Russian vessels could use its entire width, bringing them significantly closer to the coastline. If such a restriction were imposed, states enforcing the ban would also need to be prepared to physically block vessels and conduct boardings.

CONCLUSIONS AND RECOMMENDATIONS

The continuity of Estonia's critical services and economic security relies heavily on the uninterrupted operation of undersea infrastructure. Sabotage of this infrastructure can serve various strategic objectives, from disrupting government communications and military command systems in the initial stages of conflict to restricting internet access, damaging economic competitors, or causing economic disruption for geopolitical gain. Often, multiple objectives are pursued simultaneously through different tactics. Deliberate destruction of infrastructure can also be used to heighten societal anxiety and force attention onto a specific issue, thereby diverting focus from other strategic goals.

THE INADEQUATE PROTECTION OF UNDERWATER INFRASTRUCTURE CAN HAVE SEVERE CONSEQUENCES. PHOTOGRAPH: PIXABAY.COM

Due to the undersea energy connections running through the Baltic Sea, the Baltic states face a higher risk of critical service disruptions than countries on the sea's western shore. This vulnerability stems primarily from the NordBalt electricity link between Lithuania and Sweden, and the Estlink 1 and 2 interconnectors between Estonia and Finland, which connect the Baltic states to the European electricity market. Since the likelihood of deliberate attacks on undersea infrastructure has risen in recent years and is expected to remain high, planning for accelerated protective measures—along with the necessary regulatory adjustments and additional protection mechanisms—is essential. Effective protection of Estonia's and other Baltic states' subsea infrastructure requires coordinated efforts among various agencies, close collaboration with the private sector, and strong partnerships with allies—not only for prevention but also for apprehending perpetrators and ensuring rapid recovery.

Various sources indicate that Russia's hybrid tactics pose a serious threat to critical undersea infrastructure in Northern Europe, the Black Sea, the Atlantic Ocean, and other regions. In the Baltic Sea, additional risk arises from Kaliningrad, which offers Russia increased operational capability in the area. The trade routes and undersea connections linking Kaliningrad with the rest of Russia provide opportunities for covert operations against NATO countries' undersea infrastructure. Targeting critical infrastructure—including undersea assets—is a core element of Russia's military doctrine. With Russia's conventional forces engaged in Ukraine, it seeks asymmetric advantages in other sectors, particularly in the strategically vital realm of undersea infrastructure. To this end, Russia has developed and deployed, and continues to refine, its undersea reconnaissance and sabotage capabilities, operating both within its navy and under the guise of civilian oceanographic research missions.

Effective protection of Estonia's and other Baltic states' subsea infrastructure requires coordinated efforts among various agencies, close collaboration with the private sector, and strong partnerships with allies.

Complete protection of undersea infrastructure is impossible, especially without stronger public–private cooperation and better data-sharing mechanisms. Aerial surveillance and satellite imagery are key components of an undersea infrastructure protection system, as accurate threat detection requires cross-referencing acoustic signals with satellite data. Because Estonia lacks these capabilities on its own, it must develop critical undersea infrastructure protection solutions through international cooperation, including within the EU and NATO frameworks.

The European Union and NATO have intensified cooperation on protecting critical infrastructure—particularly undersea assets—following Russia's full-scale invasion of Ukraine on 24 February 2022. The sabotage of the Nord Stream gas pipelines and the destruction of the Balticconnector gas pipelines between Finland and Estonia have further heightened the urgency of this issue. In response, NATO established the Maritime Center for the Security of Critical Undersea Infrastructure under its Maritime Command (MARCOM) in the United Kingdom and created the NATO–EU Task Force on the Resilience of Critical Infrastructure, among other initiatives. As undersea infrastructure protection is still a relatively new area of collaboration, it will require continued development in the coming years, including the establishment of concrete capabilities. Estonia, which is particularly vulnerable in this domain and for whom independent capability-building would be prohibitively resource-intensive, should therefore take an active role in shaping and advancing these efforts within NATO and EU frameworks. Protecting critical undersea infrastructure is

Targeting critical infrastructure—particularly undersea assets—is a core element of Russia's military doctrine. To this end, Russia has developed and deployed, and continues to refine, its undersea reconnaissance and sabotage capabilities, operating both within its navy and under the guise of civilian oceanographic research missions.

challenging because most of it is privately owned or jointly managed, crosses multiple national jurisdictions or international waters, and has officially known locations. These factors make continuous surveillance difficult, drive up protection costs, and leave the infrastructure vulnerable—particularly considering hostile actors' hybrid strategies. The central task is therefore to establish robust national and international regulations to deter deliberate attacks.

A major challenge in protecting critical undersea infrastructure is that most of it is privately owned or shared between multiple stakeholders, crosses different national jurisdictions or extends beyond state jurisdiction into international waters, while its exact locations are publicly known. These factors make continuous surveillance difficult, protective measures costly and the infrastructure itself a potentially vulnerable target, particularly given the hybrid strategies of hostile actors. The greatest challenge is therefore to establish sufficient national and international regulations to prevent the recurrence of deliberate attacks.

Estonia and the other Baltic states must develop critical undersea infrastructure protection solutions through international cooperation, including within the EU and NATO frameworks.

Applicable legislation must effectively protect undersea connections so that perpetrators cannot act with impunity. This includes creating and expanding security zones around infrastructure and improving coastal states' ability to respond to threats or attacks. The responsibility to safeguard subsea infrastructure should extend beyond a country's exclusive economic zone to reduce opportunities for sabotage. This is especially important for Estonia in the Gulf of Finland, where a narrow stretch of sea connects two NATO countries. In cases of suspected damage, states should invoke the right of visit under Article 110(2) of the United Nations Convention on the Law of the Sea (UNCLOS). Any deliberate damage to infrastructure must be recognized as unlawful and met with strong, decisive responses.

Should a kinetic conflict or hostile posturing arise—particularly involving Kaliningrad—several non-military actions could be taken by the collective defense alliance opposing Russia to protect undersea connections. For example, Finland and Estonia could consider amending their bilateral agreement on territorial waters, which currently grants a three-nautical-mile international shipping corridor on either side of the Gulf of Finland's median line. Removing this corridor would restrict Russian vessels' access to the Gulf of Finland but would require significant changes to international maritime law. Alternatively, Denmark and Germany could limit Russian shipping through the Danish Straits and the Kiel Canal, curbing the flow of LNG tankers from Western Siberia or the Russian Far East into the Baltic Sea.

Estonia's greatest vulnerability is the simultaneous disruption of multiple connections essential for critical services. The October 2023 incidents revealed that deliberate attacks can coincide with routine maintenance or unexpected outages, posing a serious risk to electricity, gas, and data connections. Such disruptions jeopardize government operations, private businesses, and households. For this reason, risk and threat scenario analyses must focus not only on mitigating individual risks but also on examining and mitigating the potential for simultaneous failures across multiple connections and the cascading effects that could exacerbate their impact.

Legislation must effectively protect undersea connections so that perpetrators cannot act with impunity.

Given Estonia's limited capacity for dispatchable and compensatory electricity generation, power supply shortages would also lead to communication network disruptions within approximately four hours. Therefore, it remains critical to continue rais-

ing public awareness and preparedness, ensuring that local governments, essential buildings (such as schools and kindergartens), social centers, apartment buildings and residents can remain as self-sufficient as possible for up to seven days in crisis situations. Even in cases where disruptions extend beyond a week, an initial preparedness phase covering a seven-day period helps build adaptive capacity for managing prolonged crises. Additionally, risk assessments must consider not only single incidents but also the cascading effects of multiple failures.

For Estonia, the greatest risk related to undersea infrastructure is the simultaneous disruption of multiple connections essential for critical services.

A major risk to service continuity is the time needed to repair damaged undersea connections—especially if planned repairs coincide with unexpected outages—potentially leading to months-long disruptions. It is therefore critical for Estonia and other countries to secure monitoring and restoration capabilities through contracts and stockpiles of essential materials, ensuring that qualified partners can carry out inspections and repairs promptly.

It is critical for Estonia and neighboring countries to secure monitoring and restoration capabilities through contracts and stockpiles of essential materials, ensuring that qualified partners can carry out inspections and repairs promptly.

When investing in critical infrastructure, minimizing dependence on non-EU countries—especially China—is key to reducing espionage and sabotage risks. This involves avoiding Chinese technology in the defense and security sectors, reassessing procurement rules so that the lowest bid does not automatically win, and restricting companies linked to China, even if registered elsewhere.

Regulatory frameworks should incorporate lessons learned from past incidents and address how to inform the public during investigations. Such cases are not merely criminal matters; they can represent national security challenges that warrant timely and accurate communication, rather than limited disclosures typical of criminal inquiries. During recent incidents—such as the Balticconnector episode and cable disruptions with Sweden—initial information reached Estonia through Finnish and Swedish authorities and media outlets, which highlights the need for effective, direct communication channels.

When investing in critical infrastructure, minimizing dependence on non-EU countries—especially China—is key to reducing espionage and sabotage risks.

Estonia and its allies must take a firm stance that destroying undersea infrastructure is unequivocally unlawful. Responses should not be constrained by "gray zone" considerations. Quick, decisive action by NATO members around the Baltic Sea will establish a strong deterrent, helping prevent future sabotage of critical undersea infrastructure.

REFERENCES

Aedmaa, A., 2024. Intervjuu Elisa Eesti ASi peajuristi Allan Aedmaa'ga [Interview] (18.04.2024).

Alandi, A., 2025. "Välisilm" uuris, kuidas mereõigus aitaks Läänemerel korda hoida. ERR, 6 January 2025. [Online] Available at: https://www.err.ee/1609568521/valisilm-uuris-kuidas-mereoigus-aitaks-laanemerel-korda-hoida [Accessed 07.01.2025].

Anadolu Agency, 2024. Bosporus maritime traffic temporarily halted as tanker anchors. Daily Sabah. [Online] Available at: https://www.dailysabah.com/turkiye/istanbul/bosporus-maritime-traffic-temporarily-halted-as-tanker-anchors [Accessed 09.01.2025].

Andžans, M., 2021. Towards more comprehensive and interrelated infrastructure protection systems. In: Critical Infrastructure in the Baltics and Norway, M. Andžans, A. Spruds and U. Sverdrup (eds.), Latvian Institute of International Affairs: Riga.

Annual Threat Assessment, 2024. Annual Threat Assessment of the U.S. Intelligence Community. Office of the Director of National Intelligence, 5 February 2024. [Online] Available at: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf [Accessed 20.03.2024].

Aoyama, R., 2016. "One Belt, One Road": China's New Global Strategy. Journal of Contemporary East Asia Studies 5(2), 3–22. [Online] Available at: https://doi.org/10.1080/24761028.2016.11869094.

Associated Press, 2024. Russia launches massive naval drills with China. Vahendanud DefenseNews, 10 September 2024. [Online] Available at: https://www.defensenews.com/global/europe/2024/09/10/russia-launches-massive-naval-drills-with-china/ [Accessed 13.01.2025].

Aven, T., 2023. On the gap between theory and practice in defining and understanding risk. Safety Science 168 (2023) 106325. [Online] Available at: https://doi.org/10.1016/j.ssci.2023.106325.

Azaria, D. & Ulfstein, G., 2022. Are sabotage of submarine pipelines an 'armed attack' triggering a right to self-defence? EJIL:Talk!, 18 October 2022. [Online] Available at: https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/ [Accessed 02.03.2024].

Bafoutsou, G., Papaphilippou, M. & Dekker, M., 2023. Subsea cables – what is at stake? The European Union Agency for Cybersecurity. ENISA. [Online] Available at: https://op.europa.eu/et/publication-detail/-/publication/f28034a4-575c-11ee-9220-01aa75ed71a1 [Accessed 29.03.2024].

BBC, 2022. Damaged cable leaves Shetland cut off from mainland. BBC, 20 October 2022. [Online] Available at: https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-63326102 [Accessed 01.03.2024].

BNS, 2021. Eestis täisvõimsusel toodetav elekter börsihinda alla ei too. Postimees, 6 December 2021. [Online] Available at: https://majandus.postimees.ee/7402442/eestis-taisvoimsusel-toodetav-elekter-borsihinda-alla-ei-too [Accessed 10.07.2024].

Bockmann, M., 2024. Finland police seize Russian-linked dark fleet tanker Eagle S in cable-cutting investigation. Lloyd's List. [Online] Available at: https://www.lloydslist.com/LL1151950/Finland-police-seize-Russian-linked-dark-fleet-tanker-Eagle-S-in-cable-cutting-investigation [Accessed 09.01.2025].

Bouisso, J., Michel, A. & Tchoubar, P., 2024. Shell companies, ghost ships and secret traders: How Russia circumvents Western oil sanctions. Le Monde. [Online] Available at: https://www.lemonde.fr/en/les-decodeurs/article/2024/10/30/shell-companies-ghost-ships-and-secret-traders-how-russia-circumvents-western-oil-sanctions_6730981_8.html [Accessed 09.01.2025].

Brooke-Holland, L., 2023. Seabed warfare: Protecting the UK's undersea infrastructure. House of Commons Library. [Online] Available at: https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/ [Accessed 29.02.2024].

Brussels Times, 2022. Fiber optic cable sabotage causes global internet slowdown. The Brussels Times, 25 October 2022. [Online] Available at: https://www.brusselstimes.com/311704/fibre-optic-cable-sabotage-causes-global-internet-slowdown [Accessed 19.03.2024].

Brzozowski, A., 2020. NATO seeks ways of protecting undersea cables from Russian attacks. Euractiv, 23 October 2020. [Online] Available at: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/ [Accessed 29.02.2024].

Bueger, C. & Liebetrau, T., 2021. Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, Vol. 42(2), pp. 392–413. [Online] Available at: https://doi.org/10.1080/13523260.2021.1907129.

Bueger, C., Liebetrau, T. & Franken, J., 2022. Security threats to undersea communications cables and infrastructure – consequences for the EU. European Parliament. [Online] Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf [Accessed 29.02.2024].

Burdette, L., 2021. Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy. Journal of Public and International Affairs. [Online] Available at: https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy [Accessed 29.02.2024].

CCDCOE, 2019. Strategic importance of, and dependence on, undersea cables. NATO Cooperative Cyber Defence Centre of Excellence CCDCOE. [Online] Available at: https://www.ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [Accessed 29.02.2024].

China Council for the Promotion of International Trade CCPIT, 2024. Ren Hongbin. [Online] Available at: https://en.ccpit.org/infoById/b7b80d2ea05811eca0a60242ac1c0002/10 [Accessed 20.03.2024].

Citic Telecom International. Corporate Profile. [Online] Available at: https://www.citictel.com/about-us/corporate-profile/ [Accessed 19.03.2024].

Clare, M., 2021. Submarine Cable Protection and the Environment. The International Cable Protection Committee (ICPC). [Online] Available at: https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf [Accessed 01.03.2024].

Cooper, C., 2023. NATO warns Russia could target undersea pipelines and cables. Politico, 3 May 2023. [Online] Available at: https://www.politico.eu/article/nato-warns-russia-could-target-undersea-pipelines-and-cables/ [Accessed 26.02.2024].

Corera, G., 2023. Ukraine war: The Russian ships accused of North Sea sabotage. BBC News, 19 April 2023. [Online] Available at: https://www.bbc.com/news/world-europe-65309687 [Accessed 25.03.2024].

Council of the European Union, 2024. COUNCIL CONCLUSIONS on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan. 14280/23, Brussels, 24 October 2023. [Online] Available at: https://www.consilium.europa.eu/media/67499/st14280-en23.pdf [Accessed 01.04.2024].

Curtis, L., & Rasser, M., 2021. A techno-diplomacy strategy for telecommunications in the Indo-Pacific. Center for New American Security. [Online] Available at: https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2021-09/qtn_series_atechnodiplomacystrategy_web-1.pdf [Accessed 26.02.2024].

de Keyserling, A., 2023. Energy commodity prices in 2022 showed effects of Russia's full-scale invasion of Ukraine. U.S. Energy Information Administration (EIA). [Online] Available at: https://www.eia.gov/todayinenergy/detail.php?id=55059 [Accessed 03.01.2025].

Eesti Euroopa Liidu poliitika prioriteedid 2023–2025. [Online] Available at: https://www.riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/eesti-euroopa-liidu-poliitika/eesti-el-poliitika [Accessed 26.02.2024].

Eesti Vabariigi ja Soome Vabariigi vaheline territoriaalmere laiust käsitlev kokkulepe. RT II 1996, 32, 117. [Online] Available at: https://www.riigiteataja.ee/akt/13083984 [Accessed 12.02.2024].

Einmaa, I.-M., 2025. Valitsus eraldab Eesti Energiale Narva gaasijaama rajamiseks 100 miljonit eurot. ERR, 2 January 2025. [Online] Available at: https://www.err.ee/1609565773/valitsus-eraldab-eesti-energiale-narva-gaasijaama-rajamiseks-100-miljonit-eurot [Accessed 14.01.2025].

Electricity Market Act. RT I, 02.05.2024, 5. [Online] Available at: https://www.riigiteataja.ee/akt/102052024005?leiaKehtiv [Accessed 12.02.2024].

Elering, [n.d]. Eesti elektrisüsteem. [Online] Available at: https://elering.ee/book/export/html/1152 [Accessed 12.02.2024].

Elering, 2021. Eesti elektrivarustuskindluse aruanne. [Online] Available at: https://www.elering.ee/sites/default/files/2021-12/Varustuskindlus%202021%20lk.pdf [Accessed 18.03.2024].

Elering, 2023a. Eesti elektrivarustuskindluse aruanne. [Online] Available at: https://www.elering.ee/sites/default/files/2023-12/Elering_VKA_2023_WEB.pdf [Accessed 18.03.2024].

Elering, 2023b. Gaasituru käsiraamat. [Online] Available at: https://elering.ee/sites/default/files/public/Gaasituru%20k%C3%A4siraamat/Gaasituru_k2siraamat_A4_N5_FINAL.pdf [Accessed 01.03.2024].

Elering, 2023c. Eesti gaasiülekandevõrgu arengukava 2023–2032. [Online] Available at: https://elering.ee/sites/default/files/2024-03/Eesti%20gaasi%C3%BClekandev%C3%B5rgu%20arengukava%202023-2032_0.pdf [Accessed 12.02.2024].

Elering, 2024a. Eesti elektriülekandevõrgu arengukava 2024–2033. [Online] Available at: https://elering.ee/sites/default/files/public/elekter/elektris%C3%BCsteem/Eesti%20elektri%C3%BClekandev%C3%B5rgu%20arengukava%202024-2033.pdf [Accessed 01.03.2024].

Elering, 2024b. Eesti gaasiülekandevõrgu arengukava 2024–2033. [Online] Available at: https://elering.ee/sites/default/files/public/Gaas/Gaasis%C3%BCsteem/Eesti%20gaasi%C3%BClekandev%C3%B5rgu%20arengukava%202024-2033.pdf [Accessed 01.03.2024].

Elering, 2024c. Elektri tarbimine ja tootmine. [Online] Available at: https://www.elering.ee/elektri-tarbimine-ja-tootmine [Accessed 10.07.2024].

Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektriga varustamisel. Regulation. RT I, 08.12.2023, 3. [Online] Available at: https://www.riigiteataja.ee/akt/108122023003 [Accessed 01.03.2024].

Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded maagaasiga varustamisel. Regulation. RT I, 05.07.2023, 305. [Online] Available at: https://www.riigiteataja.ee/akt/105072023305 [Accessed 01.03.2024].

Elutähtsa telefoni-, mobiiltelefoni- ja andmesideteenuse kirjeldus ja toimepidevuse nõuded. Regulation. RT I, 26.02.2021, 17. [Online] Available at: https://www.riigiteataja.ee/akt/126022021017 [Accessed 01.03.2024].

Emergency Act. RT I, 06.07.2023, 33. [Online] Available at: https://www.riigiteataja.ee/akt/106072023033?leiaKehtiv [Accessed 19.03.2024].

Enefit Green, 2021. Keskkonnaaruanne 2021. Enefit Green AS Iru elektrijaam.

Enefit Green, 2022. Keskkonnaaruanne 2022. Enefit Green AS Iru elektrijaam.

Enefit Taastuvenergia OÜ & Nomine Consult OÜ, 2017. Eksperthinnang Iru Elektrijaama jäätmeenergiaploki eeldatava keskkonnamõju muutuse osas põletatava jäätmekoguse suurenemisel kütuse väiksema küttevääртuse tõttu.

Energiateollisuus, [n.d.]. Statistics on electricity. Energiateollisuus ry. [Online] Available at: https://energia.fi/tilastot/sahkotilastot/ [Accessed 03.01.2025].

ENSTO-E, 2024. Transparency Platform. [Online] Available at: https://transparency.entsoe.eu/dashboard/show [Accessed 10.07.2024].

Eriksson, K., 2023. Organisational learning without fire? Risk analyses as a basis for developing crisis management capabilities. Safety Science 163 (2023) 106144. https://doi.org/10.1016/j.ssci.2023.106144.

ERR, 2022. Siff pakub riigile kütusevarude hoiustamiseks maa-alust kompleksi Viimsis. ERR, 31 March 2022. [Online] Available at: https://www.err.ee/1608550210/siff-pakub-riigile-kutusevarude-hoiustamiseks-maa-alust-kompleksi-viimsis [Accessed 19.06.2024].

ERR, 2023a. Balti riigid leppisid kokku kiirendatud korras Vene elektrivõrgust lahkumises. ERR, 19 December 2023. [Online] Available at: https://www.err.ee/1609199482/balti-riigid-leppisid-kokku-kiirendatud-korras-vene-elektrivorgust-lahkumises [Accessed 01.03.2024].

ERR, 2023b. Soomlased leidsid Balticconnectori kahjustatud koha, puruks on ka sidekaabel. ERR, 10 October 2023. [Online] Available at: https://www.err.ee/1609127894/soomlased-leidsid-balticconnectori-kahjustatud-koha-puruks-on-ka-sidekaabel [Accessed 07.04.2024].

ERR, 2023c. Alexander Lott: sabotaaž merealuse taristu vastu on üha tavapärasem. ERR, 11 October 2023. [Online] Available at: https://www.err.ee/1609128644/alexander-lott-sabotaaz-merealuse-taristu-vastu-on-uha-tavaparasem [Accessed 07.04.2024].

ERR, 2023d. Newnew Polar Bear lõhkus gaasitoru täpselt kahe Nord Streami toru vahelt. ERR, 15 November 2023. [Online] Available at: https://www.err.ee/1609165783/newnew-polar-bear-lohkus-gaasitoru-tapselt-kahe-nord-streami-toru-vahelt [Accessed 02.01.2025].

ERR, 2024a. Elering tuvastas EstLink 2 rikkekoha, parandustööd kestavad augusti lõpuni. ERR, 1 March 2024. [Online] Available at: https://www.err.ee/1609269423/elering-tuvastas-estlink-2-rikkekoha-parandustood-kestavad-augusti-lopuni [Accessed 01.03.2024].

ERR, 2024b. Balticconnector peaks taas kasutusse minema 22. aprillil. ERR, 4 April 2024. [Online] Available at: https://www.err.ee/1609302528/balticconnector-peaks-taas-kasutusse-minema-22-aprillil [Accessed 07.04.2024].

ERR, 2024c. Enefit Power konserveerib Balti elektrijaama koostootmisploki. ERR, 28 March 2024. [Online] Available at: https://www.err.ee/1609296924/enefit-power-konserveerib-balti-elektrijaama-koostootmisploki [Accessed 10.07.2024].

ERR, 2024d. Michal: merevägi asub kriitilist taristut aktiivsemalt valvama ja seirama. ERR, 26 December 2024. [Online] Available at: https://www.err.ee/1609560757/michal-merevagi-asub-kriitilist-taristut-aktiivsemalt-valvama-ja-seirama [Accessed 02.01.2025].

ERR, 2024e. Koort: Eesti võinuks Balticconnectori lõhkumise uurimisel jõulisem olla. ERR, 21 August 2024. [Online] Available at: https://www.err.ee/1609430164/koort-eesti-voinuks-balticconnectori-lohkumise-uurimisel-joulisem-olla [Accessed 05.01.2025].

ERR, 2024f. Taani merevägi jälgib purunenud kaablite läheduses viibinud Hiina laeva. ERR, 20 November 2024 [Online] Available at: https://www.err.ee/1609527172/taani-merevagi-jalgib-purunenud-kaablite-laheduses-viibinud-hiina-laeva [Accessed 10.01.2025].

ERR, 2024g. Eksperdid: sidekaablid lõhkunud laeva pardale minemise peamine takistus mereõigus. ERR, 21 November 2024 [Online] Available at: https://www.err.ee/1609528453/eksperdid-sidekaablid-lohkunud-laeva-pardale-minemise-peamine-takistus-mereoigus [Accessed 10.01.2025].

ERR, 2025. Kaablikahjustamises kahtlustatav Vezhen kuulub Hiina riigile. ERR, 27. January 2025 [Online] Available at: https://www.err.ee/1609587887/kaablikahjustamises-kahtlustatav-vezhen-kuulub-hiina-riigile [Accessed 28.01.2025].

Estonian Stockpiling Agency, 2024. Eesti Varude Keskuse saamislugu. [Online] Available at: https://varudekeskus.ee/ettevottest/tegevuspohimotted/ettevotte-ajaloost [Accessed 19.06.2024].

Euractiv, 2015. Russia accused of disrupting new energy link between Sweden and Lithuania. Euractiv Media Network BV, 4 May 2015. [Online] Available at: https://www.euractiv.com/section/global-europe/news/russia-accused-of-disrupting-new-energy-link-between-sweden-and-lithuania/ [Accessed 20.03.2024].

European Commission, 2024a. Komisjon tutvustab uusi tuleviku digitaristute algatusi. Euroopa Komisjon pressiteade, 21 February 2024. [Online] Available at: https://ec.europa.eu/commission/presscorner/detail/et/IP_24_941 [Accessed 01.04.2024].

European Commission, 2024b. Comission recommendation of 26.2.2024 on secure and resislient submarine cable infrastructures. C(2023)1181, Brussels, 26 February 2024. [Online] Available at: https://digital-strategy.ec.europa.eu/et/library/recommendation-security-and-resilience-submarine-cable-infrastructures [Accessed 01.04.2024].

European Commission, 2024c. White paper. How to master Europe's digital infrastructure needs? COM(2024)81, Brussels, 21 February 2024. [Online] Available at: https://digital-strategy.ec.europa.eu/et/library/white-paper-how-master-europes-digital-infrastructure-needs [Accessed 01.04.2024].

European Union, 2023. Tõhustatud EL-i merendusjulgeoleku strateegia muutuvate merendusohtudega toimetulekuks. Ühisteatis Euroopa Parlamendile ja Nõukogule, Brussels, 10 March 2023, JOIN(2023) 8 final. [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0008 [Accessed 25.03.2024].

European Parliament, 2022. ELi kriitilise tähtsusega taristu kaitse. EP täiskogu uudiskiri 17–20 October 2022. [Online] Available at: https://www.europarl.europa.eu/news/et/agenda/briefing/2022-10-17/2/eli-kriitilise-tahtsusega-taristu-kaitse [Accessed 22.02.2024].

European Parliament, 2024. Euroopa Parlamendi 17. jaanuari 2024. aasta resolutsioon Hiina mõjust Euroopa Liidu elutähtsale taristule tuleneva julgeoleku- ja kaitsealase mõju kohta (2023/2072(INI)). P9_TA(2024)0028. [Online] Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_ET.html [Accessed 22.02.2024].

Fastrup, N., Quass, L. & Thim, F. H. L., 2023. Afsløring: Russiske spionskibe forbereder mulig sabotage mod havvindmøller, gasrør og strømkabler i Danmark og Norden. DR, 19 April 2023. [Online] Available at: https://www.dr.dk/nyheder/indland/moerklagt/afsloering-russiske-spionskibe-forbereder-mulig-sabotage-mod [Accessed 25.03.2024].

Fouda, M., 2024. Finland investigates Russian 'shadow fleet' ship over Baltic Sea cable damage. Euronews, 26 December 2024. [Online] Available at: https://www.euronews.com/my-europe/2024/12/26/undersea-power-cable-linking-finland-and-estonia-suffers-damage-in-latest-baltic-sea-incid [Accessed 02.01.2025].

Frascà, D. & Galantini, L., 2023. The Issue of Submarine Cable Security. Towards a New European Security Architecture, p. 51. [Online] Available at: https://liberalforum.eu/wp-content/uploads/2023/06/BOURCHIER_ELF_New_European_Security.pdf#page=58 [Accessed 22.02.2024].

French Ministry of Armed Forces, 2022. Seabed Warfare Strategy. [Online] Available at: https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf [Accessed 22.02.2024].

Fridbertsson, N. T., 2023. Protecting Critical Maritime Infrastructure – The Role of Technology. General Report. 032 STC 23 E. NATO Parliamentary Assembly: Science and Technology Committee (STC). [Online] Available at: https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc [Accessed 21.03.2024].

Galeotti, M., 2019. The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy. Marshall Center Security Insight, No. 27. [Online] Available at: https://www.marshallcenter. org/en/publications/security-insights/baltic-states-targets-and-levers-role-regionrussian-strategy-0 [Accessed 22.02.2024].

Gallagher, J. C., 2022. Undersea Telecommunication Cables: Technology Overview and Issues for Congress. Congressional Research Service. [Online] Available at: https://crsreports.congress.gov/product/pdf/R/R47237 [Accessed 29.02.2024].

Gavin, G., 2024. Clamp down on Russian shadow fleet after tanker oil spill, says Latvia. POLITICO. [Online] Available at: https://www.politico.eu/article/russia-shadow-fleet-tanker-oil-spill-black-sea-latvia/ [Accessed 09.01.2025].

Gehringer, F. A., 2023. Undersea cables as critical infrastructure and geopolitical power tool. Konrad-Adenauer-Stiftung, No. 495. [Online] Available at: https://www.kas.de/documents/252038/22161843/Undersea+cables.pdf/aee8e59b-96dc-bc05-18ac-b1070eb76bc1 [Accessed 29.02.2024].

Geri, M., 2023. South China Sea tensions conceal a secret war to control the world's Internet. Euractiv, 2 May 2023. [Online] Available at: https://www.euractiv.com/section/china/opinion/south-china-sea-tensions-conceal-a-secret-war-to-control-the-worlds-internet/ [Accessed 29.02.2024].

Glette-Iversen, I., Flage. R. & Aven, T., 2024. Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty. Safety Science 168 (2023) 106317. https://doi.org/10.1016/j.ssci.2023.106317.

Glette-Iversen, I. & Flage, R., 2024. On unpredictable events in risk analysis. Safety Science 180 (2024) 106652. https://doi.org/10.1016/j.ssci.2024.106652.

Granlund, J. & Velizelos, A., 2023. Finländsk polis pekar ut „intressant" ryskt fartyg – färdades över förstörd svensk kabel. SVT Nyheter, 18 October 2023. [Online] Available at: https://www.svt.se/nyheter/inrikes/misstankt-ryskt-fartyg-over-trasiga-undervattenskabeln [Accessed 20.03.2024].

Green, M. A., 2024. China and Russia: Quietly Going Steady? The Wilson Center, 29 October 2024). [Online] Available at: https://www.wilsoncenter.org/blog-post/china-and-russia-quietly-going-steady [Accessed 13.01.2024].

Guilfoyle, D., Paige, T. P. & McLaughlin, R., 2022. The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables. International and Comparative Law Quarterly, Vol. 71(3), pp. 657–696. https://doi.org/10.1017/S0020589322000227.

Hendriks, M. S. & Halem, H., 2024. From space to seabed: Protecting the UK's undersea cables from hostile actors. UK: Policy Exchange. [Online] Available at: https://

policyexchange.org.uk/wp-content/uploads/From-space-to-seabed.pdf [Accessed 19.03.2024].

Hou, L-L. A., Goodwin, A., Chernova, A. & Cotovio, V., 2023. Fleet of Russian spy ships has been gathering intelligence in Nordic waters, investigation finds. CNN, 20 April 2023. [Online] Available at: https://edition.cnn.com/2023/04/19/europe/russia-spy-ships-nordic-waters-intl/index.html [Accessed 25.03.2024].

Humpert, M., 2022. Nord Stream Pipeline Sabotage Mirrors Svalbard Cable Incident. High North News, 20 September 2022. [Online] Available at: https://www.high-northnews.com/en/nord-stream-pipeline-sabotage-mirrors-svalbard-cable-incident [Accessed 01.03.2024].

Insikt Group, 2023. The Escalating Global Risk Environment for Submarine Cables. [Online] Available at: https://www.recordedfuture.com/escalating-global-risk-environment-submarine-cables [Accessed 29.02.2024].

Interfax, 2023. China's NewNew Shipping Line planning to send five transit cargo ships through the Northern Sea Route during the 2023 navigation season. [Online] Available at: https://interfax.com/newsroom/top-stories/92332/ [Accessed 06.03.2024].

Известия, 2024. Военный эксперт объяснил значение Калининграда в случае конфликта НАТО [Online] Available at: https://archive.ph/iqYrc [Accessed 24.04.2024].

Janda, J. & Corera, J., 2024. Baltic subsea sabotage: We're letting Russia (and China) undertake target practice. The Strategist, 31 December 2024. [Online] Available at: https://www.aspistrategist.org.au/baltic-subsea-sabotage-were-letting-russia-and-china-undertake-target-practice/ [Accessed 13.01.2025].

Justiits- ja digiministeerium, 2025. Eesti karmistab karistusõigust merekaablite ja torujuhtmete kaitseks. [Online] Justiits- ja digiministeerium. 10 January 2025. [Online] Available at: https://www.justdigi.ee/uudised/eesti-karmistab-karistusoigust-merekaablite-ja-torujuhtmete-kaitseks [Accessed 10.01.2025].

Kaitsepolitseiamet, 2009. Aastaraamat 2008. [Online] Available at: https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2008.pdf [Accessed 10.01.2025].

Kaitsepolitseiamet, 2024. Aastaraamat 2023–2024. [Online] Available at: https://kapo.ee/sites/default/files/content_page_attachments/Aastaraamat%202023-2024.pdf [Accessed 12.04.2024].

Kaitseväe korralduse seadus. RT I, 21.06.2024, 14. [Online] Available at: https://www.riigiteataja.ee/akt/127012023003?leiaKehtiv [Accessed 06.03.2024].

Kaitseväe põhimäärus. Regulation. RT I, 28.06.2023, 13. [Online] Available at: https://www.riigiteataja.ee/akt/128062018008?leiaKehtiv [Accessed 06.03.2024].

Kaitsevägi, 2024. Liitlased tegelevad Läänemerel veealuse taristu kaitse ja turvalisuse tagamisega. Kaitseväe Peastaap, 3 June 2024. [Online] Available at: https://mil.ee/uudised/liitlased-tegelevad-laanemerel-veealuse-taristu-kaitse-ja-turvalisuse-tagamisega [Accessed 02.01.2025].

Katinas, P., 2024. April 2024 — Monthly analysis of Russian fossil fuel exports and sanctions. Centre for Research on Energy and Clean Air. 20 May 2024. [Online] Available at: https://energyandcleanair.org/april-2024-monthly-analysis-of-russian-fossil-fuel-exports-and-sanctions/ [Accessed 09.01.2025].

Katinas, P. & Wickenden, L., 2024. Ensuring an ecological disaster: 'Shadow' tanker spill could cost coastal states USD 1.6 bn. Centre for Research on Energy and Clean Air. [Online] Available at: https://energyandcleanair.org/publication/ensuring-an-ecological-disaster-shadow-tanker-spill-could-cost-coastal-states-usd-1-6-bn/ [Accessed 03.01.2025].

Kaushal, S., 2023. Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure. The Royal United Services Institute for Defence and Security RUSI. [Online] Available at: https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure [Accessed 29.02.2024].

Keskkonnaamet, 2024. Menetlus M-126224. Taotlus T-KL/1019996-3. KOTKAS. Keskkonnaotsuste Infosüsteem. [Online] Available at: https://kotkas.envir.ee/permits/public_application_details?represented_id=&proceeding_id=26790&application_id=1022466 [Accessed 19.06.2024].

Kilumets, M., Teppan, S., 2024. Patrull-laev Raju läks Estlink 1 turvama. ERR, 27 December 2024. [Online] Available at: https://www.err.ee/1609561075/patrull-laev-raju-laks-estlink-1-turvama [Accessed 02.01.2025].

Kirk, L., 2022. Mysterious Atlantic cable cuts linked to Russian fishing vessels. EUobserver. 26 October 2022. [Online] Available at: https://euobserver.com/nordics/156342 [Accessed 01.03.2024].

Kivi, L., 2024. Soome võimud hoidsid ära ka Estlink 1 ja Balticconnectori lõhkumise. Delfi, 28 December 2024. [Online] Available at: https://www.delfi.ee/artikkel/120346324/soome-voimud-hoidsid-ara-ka-estlink-1-ja-balticconnectori-lohkumise [Accessed 02.01.2025].

Kliimaministeerium, 2024. Eesti ja Soome tõhustavad koostööd merealuse energiataristu vallas. Kliimaministeerium, 27.09.2024. [Online] Available at: https://kliimaministeerium.ee/uudised/eesti-ja-soome-tohustavad-koostood-merealuse-energiataristu-vallas [Accessed 03.01.2025].

Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Edmonds, J. & Wallet, J., 2021. Russian Military Strategy: Core Tenets and Operational Concepts. CNA. [Online] Available at: https://www.cna.org/reports/2021/10/Russian-Military%20-Strategy-Core-Tenets-and-Operational-Concepts.pdf [Accessed 19.02.2024].

Koppel, K., 2024. Balti riikide elektritarbimine toetub 40 protsendi ulatuses impordile. ERR, 22 November 2024. [Online] Available at: https://www.err.ee/1609527271/balti-riikide-elektrivarustus-toetub-40-protsendi-ulatuses-impordile [Accessed 03.01.2025].

Kreek, R., 2024. Rootsi paljastab, kes Nord Streami õhku lasi. Postimees, 6 February 2024. [Online] Available at: https://majandus.postimees.ee/7954316/rootsi-paljastab-kes-nord-streami-ohku-lasi [Accessed 15.02.2024].

Kressa, K., 2024. Arestitud Vene tankerlaeval käib ööpäevaringne uurimine. Meeskonnaks on Gruusia ja India kodanikud. Delfi, 29 December 2024. [Online] Available at: https://www.delfi.ee/artikkel/120346463/arestitud-vene-tankerlaeval-kaib-oopaevaringne-uurimine-meeskonnaks-on-gruusia-ja-india-kodanikud [Accessed 02.01.2025].

Kulleste, H-M., 2025. VIDEO JA KAART | Kaablilõhkumises kahtlustataval laeval paistab olevat viga saanud ankur. Laeva külastas Rootsi julgeolek. Delfi, 27. January 2025. [Online] Available at: https://www.delfi.ee/artikkel/120352628/

video-ja-kaart-kaablilohkumises-kahtlustataval-laeval-paistab-olevat-viga-saanud-ankur-laeva-kulastas-rootsi-julgeolek [Accessed 28.01.2025].

Kumar, R., 2023. Securing the Digital Seabed: Countering China's Underwater Ambitions. Journal of Indo-Pacific Affairs, pp. 74–90. [Online] Available at: https://media.defense.gov/2023/Nov/14/2003340185/-1/-1/1/FEATURE%20KUMAR%20-%20JIPA.PDF [Accessed 29.02.2024].

Kuszynski, S. & Barns, G., 2022. The Geopolitics of Undersea Cables: Underappreciated and Under Threat. London Politica, at 8-9. [Online] Available at: https://static1.squarespace.com/static/5efb88803e2328745c7b3c39/t/639f7e25ba5e494096dd02ac/1671396903006/Geopolitics+of+Undersea+Cables.pdf [Accessed 19.02.2024].

Lauri, V., 2023. USA ja Eesti merevägi suurendavad Eesti rannikualadel mereteadlikkust. ERR, 5 May 2023. [Online] Available at: https://www.err.ee/1608969307/usa-ja-eesti-merevagi-suurendavad-eesti-rannikualadel-mereteadlikkust [Accessed 20.02.2024].

Levi, I., 2024. January 2024 — Monthly analysis of Russian fossil fuel exports and sanctions. Centre for Research on Energy and Clean Air. 14 February 2024 [Online] Available at: https://energyandcleanair.org/january-2024-monthly-analysis-of-russian-fossil-fuel-exports-and-sanctions/ [Accessed 09.01.2025].

Li, M., 2023. First Arctic liner link with China started by New New Shipping. The Loadstar. 26 July 2023. [Online] Available at: https://theloadstar.com/first-arctic-liner-link-with-china-started-by-new-new-shipping/ [Accessed 20.03.2024].

Lima, J. & Drozdiak, N., 2023. NATO Turns to Underwater Drones and AI in Bid to Deter Russia. Bloomberg News, 28 September 2023. [Online] Available at: https://www.bnnbloomberg.ca/nato-turns-to-underwater-drones-and-ai-in-bid-to-deter-russia-1.1977397 [Accessed 29.02.2024].

Loik, R., 2024. Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation. Journal on Baltic Security, Vol. 10(2), pp. 1–25. DOI: 10.57767/jobs_2024_008

Lomp, L-E., 2024. Paet kaabli rikkest: Venemaa ja Hiina testivad, kas ja mida EL ja NATO ette võtavad. Postimees, 26 December 2024. [Online] Available at: https://www.postimees.ee/8161145/paet-kaabli-rikkest-venemaa-ja-hiina-testivad-kas-ja-mida-el-ja-nato-ette-votavad [Accessed 05.01.2025].

Long, M. L., 2023. Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks. U.S. Naval Institute Proceedings, Vol. 149/5/1,443. [Online] Available at: https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks [Accessed 29.02.2024].

Lott, A., 2023a. Attacks against Europe's Offshore Infrastructure within and beyond the Territorial Sea under Jus ad Bellum. EJIL:Talk!, 17 October 2023. [Online] Available at: https://www.ejiltalk.org/attacks-against-europes-offshore-infrastructure-within-and-beyond-the-territorial-sea-under-jus-ad-bellum/ [Accessed 02.03.2024].

Lott, A., 2023b. Alexander Lott: kas Eesti või Soome saanuks arestida NewNew Polar Beari? ERR, 4 November 2023. [Online] Available at: https://www.err.ee/1609153672/alexander-lott-kas-eesti-voi-soome-saanuks-arestida-newnew-polar-beari [Accessed 02.03.2024].

Madsen, T., 2024. Läänemere veealuste kaablite purustamise kahtlusalune on Hiina laev. Postimees, 19 November 2024. [Online] Available at: https://maailm.postimees.ee/8137870/laanemere-veealuste-kaablite-purustamise-kahtlusalune-on-hiina-laev [Accessed 05.01.2025].

MarineTraffic.com, 2024. Vessel Characteristics: Ship NEWNEW POLAR BEAR (Container Ship) Registered in Hong Kong – Vessel details, Current position and Voyage information - IMO 9313204MMSI 9313204 Call Sign VRVQ4. [Online] Available at: https://www.marinetraffic.com/en/ais/details/ships/shipid:3162/mmsi:477893800/imo:9313204/vessel:NEWNEW POLAR BEAR [Accessed 20.03.2024].

Maritime Executive, 2025. "Dark Fleet" Tanker Faces Civil and Criminal Cases in Finland. The Maritime Executive. [Online] Available at: URL https://maritime-executive.com/article/suspect-dark-fleet-tanker-faces-civil-and-criminal-actions-in-finland [Accessed 10.01.2025].

Mauldin, A., 2023. Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic? TeleGeography, 4 May 2023. [Online] Available at: https://blog.telegeography.com/2023-mythbusting-part-3 [Accessed 02.03.2024].

Mehvar, S., Wijnberg, K., Borsje, B., Kerle, N., Schraagen, J. M., Vinke-de Kruijf, J., Geurs, K., Hartmann, R., Hogeboom, R. & Hulscher, S., 2021. Review article: Towards resilient vital infrastructure systems – challenges, opportunities, and future research agenda. Nat. Hazards Earth Syst. Sci., 21, 1383–1407. https://doi.org/10.5194/nhess-21-1383-202.

Mereväe põhimäärus. Kinnitatud Kaitseväe juhataja 25.01.2024 käskkirjaga nr 154. [Online] Available at: https://mil.ee/wp-content/uploads/2024/01/20231026_A_KV_Merev_e_p_him__rus.pdf [Accessed 20.03.2024].

Milne, R., 2024. Finland seizes Russian shadow fleet oil tanker after cable-cutting incident. Financial Times. [Online] Available at: https://www.ft.com/content/0c208ac1-f416-41b2-a373-ec7f90b84ca8 [Accessed 09.01.2025].

Monaghan, S., Svendsen, O., Darrah, M. & Arnold, E., 2023. NATO's Role in Protecting Critical Undersea Infrastructure. Center for Strategic and International Studies CSIS. [Online] Available at: https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure [Accessed 29.02.2024].

Nakamura, H., 2023. The Enemy Below: Fighting against Russia's Hybrid Underwater Warfare. Center for Maritime Strategy. [Online] Available at: https://centerformaritimestrategy.org/publications/the-enemy-below-fighting-against-russias-hybrid-underwater-warfare/ [Accessed 29.02.2024].

NATO, 2023a. NATO and the EU set up taskforce on resilience and critical infrastructure. 11 January 2023. [Online] Available at: https://www.nato.int/cps/en/natohq/news_210611.htm [Accessed 29.02.2024].

NATO, 2023b. NATO and European Union launch task force on resilience of critical infrastructure. 16 March 2023. [Online] Available at: https://www.nato.int/cps/en/natohq/news_212874.htm [Accessed 19.03.2024].

NATO, 2023c. NATO Secretary General addresses protection of critical undersea infrastructure, support to Ukraine with EU Defence Ministers. 14 November 2023. [Online] Available at: https://www.nato.int/cps/en/natohq/news_220058.htm [Accessed 29.02.2024].

NATO, 2025. NATO launches “Baltic Sentry” to increase critical infrastructure security. 14 January 2025. [Online] Available at: https://www.nato.int/cps/en/natohq/news_232122.htm#:~:text=NATO%20will%20work%20within%20the,the%20importance%20of%20robust%20enforcement [Accessed 14.01.2025].

Natural Gas Act. RT I, 02.05.2024, 8. [Online] Available at: https://www.riigiteataja.ee/akt/261477?leiaKehtiv [Accessed 29.02.2024].

Newdick, T., 2021. Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut. The WarZone, 11th of November 2021. [Online] Available at: https://www.twz.com/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut [Accessed 29.02.2024].

Nolan-McSweeney, M., Ryan, B. & Cobb, S., 2023. Interviews with rail industry leaders about systems thinking in the management of organisational change and risk management. Safety Science 164 (2023) 106168. https://doi.org/10.1016/j.ssci.2023.106168.

NSR General Administration ROSATOM, 2023a. РАЗРЕШЕНИЕ № 557/5. [Online] Available at: https://nsr.rosatom.ru/upload/iblock/f26/r-Newnew-polar-bear-06.07.2023.pdf [Accessed 20.03.2024].

NSR General Administration ROSATOM, 2023b. РАЗРЕШЕНИЕ № Р075-00172- 77/00740677. [Online] Available at: https://nsr.rosatom.ru/upload/iblock/5e5/203727603_r-Newnew-polar-bear_signed.pdf [Accessed 20.03.2024].

Paadik, I., 2024. Eesti elanike teadlikkus ning valmisolek siseturvalisuse valdkonda puudutavate pikaajaliste kriisidega toimetulekuks. Magistritöö. Tallinn: Sisekaitseakadeemia.

Päästeamet, 2023. Elanikkonna hädaolukorraks valmisoleku alase teadlikkuse indeksuuring 2023. [Online] Available at: https://www.rescue.ee/files/Uuringud/2023-elanikkonna-hadaolukorraks-valmisoleku-alase-teadlikkuse-indeksuuring.pdf?fc9a1cadb4 [Accessed 02.04.2024].

Page, M., 2023. Russia, a Chinese cargo ship and the sabotage of subsea cables in the Baltic Sea. The Strategist, 31 October 2023. [Online] Available at: https://www.aspistrategist.org.au/russia-a-chinese-cargo-ship-and-the-sabotage-of-subsea-cables-in-the-baltic-sea/ [Accessed 29.02.2024].

Pancevski, M., 2024. Brush With Russia in Baltic Points to New Flashpoint in NATO-Moscow Shadow War. The Wall Street Journal, 15 December 2024. [Online] Available at: https://www.wsj.com/world/europe/brush-with-russia-in-baltic-points-to-new-flashpoint-in-nato-moscow-shadow-war-08b5b182 [Accessed 05.01.2025].

Pau, A., 2023. Must stsenaarium. Kas Eesti riigil on olemas plaan, kui lõigataks läbi kõik merealused sidekaablid? Forte, 23 October 2023. [Online] Available at: https://forte.delfi.ee/artikkel/120241767/must-stsenaarium-kas-eesti-riigil-on-olemas-plaan-kui-loigataks-labi-koik-merealused-sidekaablid [Accessed 20.02.2024].

Pillai, H., 2023. Protecting Europe’s critical infrastructure from Russian hybrid threats. Centre for European Reform. [Online] Available at: https://www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid [Accessed 29.02.2024].

Pollet, M., 2023. EU looks to boost secure submarine internet cables in 2024. Politico, 11 October 2023. [Online] Available at: https://www.politico.eu/article/eu-looks-to-boost-secure-submarine-internet-cables-in-2024/ [Accessed 29.02.2024].

Pollet, M., 2024. Underwater SOS: EU wants to defend subsea cables. Politico, 16 February 2024. [Online] Available at: https://www.politico.eu/article/eu-subsea-data-cable-interconnector-security/ [Accessed 29.02.2024].

Põlluste, G., 2022. Eestit välisilmaga ühendavad torud ja kaablid on rahvusvahelistes vetes haavatavad. Delfi, 1 October 2022. [Online] Available at: https://www.delfi.ee/artikkel/120075740/kaart-eestit-valisilmaga-uhendavad-torud-ja-kaablid-on-rahvusvahelistes-vetes-haavatavad [Accessed 20.02.2024].

Postimees, 2016. Väidetavalt ajas Putini lähikondlane ISISega naftaäri. Postimees, 13 May 2016. [Online] Available at: https://majandus.postimees.ee/3693195/vaidetavalt-ajas-putini-lahikondlane-isisega-naftaari [Accessed 20.03.2024].

Postimees, 2023. BALTICCONNECTOR – Stoltenberg lubas võimalikule rünnakule ühtset NATO vastust. Postimees, 11 October 2023. [Online] Available at: https://maailm.postimees.ee/7873516/balticconnector-stoltenberg-lubas-voimalikule-runnakule-uhtset-nato-vastust [Accessed 20.02.2024].

Postimees, 2024a. Rootsi lõpetas Nord Streami plahvatuste uurimise. Postimees, 7 February 2024. [Online] Available at: https://majandus.postimees.ee/7954987/rootsi-lopetas-nord-streami-plahvatuste-uurimise [Accessed 20.02.2024].

Postimees, 2024b. Riigikaitsekomisjoni sõnul on vaja merealuse taristu kaitsmiseks jõulisi samme. Postimees, 27 December 2024. [Online] Available at: https://www.postimees.ee/8161961/riigikaitsekomisjoni-sonul-on-vaja-merealuse-taristu-kaitsmiseks-joulisi-samme [Accessed 02.01.2025].

Prokuratuur, 2006. Valmisid tankerilt Flawless võetud proovide esialgsed tulemused 07.03.2006 [Online] Available at: https://www.prokuratuur.ee/uudised/valmisid-tankerilt-flawless-voetud-proovide-esialgsed-tulemused [Accessed 10.01.2025].

Pulk, M., 2022. Ministeerium: mereala kaitstakse samamoodi nagu riigipiiri. Postimees, 17 October 2022. [Online] Available at: https://www.postimees.ee/7628074/ministeerium-mereala-kaitstakse-samamoodi-nagu-riigipiiri [Accessed 20.02.2024].

Radin, A., 2017. Hybrid Warfare in the Baltics. Threats and potential responses. RAND Corporation. [Online] Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf [Accessed 20.02.2024].

Raghunandan, V., 2024a. May 2024 — Monthly analysis of Russian fossil fuel exports and sanctions. Centre for Research on Energy and Clean Air. 24 June 2024. [Online] Available at: https://energyandcleanair.org/may-2024-monthly-analysis-of-russian-fossil-fuel-exports-and-sanctions/ [Accessed 09.01.2025].

Raghunandan, V., 2024b. October 2024 — Monthly analysis of Russian fossil fuel exports and sanctions. Centre for Research on Energy and Clean Air. 8 November 2024. [Online] Available at: https://energyandcleanair.org/october-2024-monthly-analysis-of-russian-fossil-fuel-exports-and-sanctions/ [Accessed 09.01.2025].

Randveer, K. J., 2024. Eesti Energia avaldas, kui suurt mõju on avaldanud EstLink 2 rike elektrihinnale. Delfi Ärileht, 12 August 2024. [Online] Available at: https://arileht.delfi.ee/artikkel/120314135/eesti-energia-avaldas-kui-suurt-moju-on-avaldanud-estlink-2-rike-elektrihinnale [Accessed 03.01.2025].

Reuters, 2024. US Sanctions UAE Shipping Firm for Violating Russian Crude Oil Price Cap. Voice of America. [Online] Available at: https://www.voanews.com/a/

us-sanctions-uae-shipping-firm-for-violating-russian-crude-oil-price-cap/7445471.html [Accessed 09.01.2025].

Riibon, A., 2024. Intervjuu Eesti Mereväe mereoperatsioonide keskuse ülema Ardo Riibon'iga [Interview] (22.03.2024).

Riigikontroll, 2025. Elektriga varustavate objektide turvalisus. Riigikontrolli aruanne Riigikogule. Tallinn, 9 January 2025. [Online] Available at: https://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/557GetPage/1/557Year/-1/ItemId/2475/amid/557/language/et-EE/Default.aspx [Accessed 15.01.2025].

Ringstrom, A. & Solsvik, T., 2022. Nord Stream leaks confirmed as sabotage, Sweden says. Reuters, 18 November 2022. [Online] Available at: https://www.reuters.com/world/europe/traces-explosives-found-nord-stream-pipelines-sweden-says-2022-11-18/ [Accessed 02.03.2024].

ROSATOM FLOT, 2012. Atomic lighter "Sevmorput". [Online] Available at: https://web.archive.org/web/20120426002347/http://www.rosatomflot.ru/index.php?menuid=34&lang=en [Accessed 20.03.2024].

Российско-Китайский деловой совет, 2024a. О Совете. [Online] Available at: https://rcbc.ru/ru/about/ [Accessed 20.03.2024].

Российско-Китайский деловой совет, 2024b. ООО „Торгмолл." [Online] Available at: https://rcbc.ru/ru/council/ooo-torgmoll/ [Accessed 20.03.2024].

Roy, S., 2018. Protecting Undersea Cables: An Underrated Element of International Cybersecurity. Cambridge International Law Journal. [Online] Available at: https://cilj.co.uk/2018/02/02/protecting-undersea-cables-an-underrated-element-of-international-cybersecurity/ [Accessed 29.02.2024].

Rozhkov-Yuryevsky, Y., 2013. The concepts of enclave and exclave and their use in the political and geographical characteristic of the Kaliningrad region. Baltic Region, 16(2), pp. 113–123. https://doi.org/10.5922/2079-8555-2013-2-11.

Ryzhenko, A., 2022. Nord Stream Explosions: Russian Sabotage in the Baltic? Eurasia Daily Monitor, 19(146). The Jamestown Foundation. [Online] Available at: https://jamestown.org/program/nord-stream-explosions-russian-sabotage-in-the-baltic/ [Accessed 23.03.2024].

Saar, P., 2024. Intervjuu Riigikantselei julgeoleku ja riigikaitse koordinatsioonidirektori asetäitja Priit Saarega [Interview] (25.04.2024).

Sajari, P., 2024. HS:n tiedot: Aseistautuneet valmiusjoukot lähetettiin keskellä yötä Eagle S -alukselle, kun syyttäjä pohti vielä terrorismia. Helsingin Sanomat, 26 December 2024. [Online] Available at: https://www.hs.fi/suomi/art-2000010927044.html [Accessed 02.01.2025].

Sanger, D. E. & Schmitt, E., 2015. Russian Ships Near Data Cables Are Too Close for U.S. Comfort. The New York Times, 25 October 2015. [Online] Available at: https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0 [Accessed 19.03.2024].

Savimaa, R. & Kont, K.-R., 2023. Kogukonnaseltside roll ja võimekus kogukondade kerksuse tagamisel kriisides. Turvalisuskompass, 2023, 4. Tallinn: Sisekaitseakadeemia, pp. 69–108.

Savimaa, R., 2024a. Muuga elanike kriisivalmidus. Uuringuraport. Tallinn: CESERE. DOI: https://doi.org/10.5281/zenodo.13341130.

Savimaa, R., 2024b. Harku valla elanike kriisivalmidus. Uuringuraport. Tallinn: CESERE. DOI: https://doi.org/10.5281/zenodo.12742427.

Schadlow, N. & Helwig, B., 2020. Protecting undersea cables must be made a national security priority. [Online] Available at: https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/ [Accessed 08.03.2024].

Scott, M., 2022. Will Russia attack undersea internet cables next? Politico, 29 September 2022. [Online] Available at: https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/ [Accessed 29.02.2024].

Shadow Fleet, 2025. War & Sanctions. [Online] Available at: https://war-sanctions.gur.gov.ua/en/transport/shadow-fleet [Accessed 09.01.2025].

SHAPE, 2025. Baltic Sentry to enhance NATO's presence in the Baltic Sea. 14 January 2025. [Online] Available at: https://shape.nato.int/news-releases/baltic-sentry-to-enhance-natos-presence-in-the-baltic-sea [Accessed 14.01.2025].

Siebold, S., 2023. NATO says Moscow may sabotage undersea cables as part of war on Ukraine. Reuters, 3 May 2023. [Online] Available at: https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/ [Accessed 29.02.2024].

Skopljak, N., 2023. Tenders canceled for Poland-Lithuania submarine interconnector. Offshore Energy, 15 May 2023. [Online] Available at: https://www.offshore-energy.biz/tenders-canceled-for-poland-lithuania-submarine-interconnector/ [Accessed 02.06.2024].

Sõmer, T., Lorenz, B., Mäses, S. & Muulmann, T., 2019. Küberkaitse. [Online] Available at: https://web.htk.tlu.ee/digitaru/kyberkaitse/ [Accessed 19.03.2024].

Soone, P., 2024. Intervjuu Elering ASi riskijuhi Peep Soonega [Interview] (09.04.2024).

Sprenger, S., 2019. Estonian intelligence flags Russian civilian vessels as would-be spy ships. Defense News, 13 March 2019. [Online] Available at: https://www.defensenews.com/global/europe/2019/03/13/estonian-intelligence-flags-russian-civilian-vessels-as-would-be-spy-ships/ [Accessed 19.03.2024].

Statistics Poland, 2024. Consumption of fuels and energy carriers in 2023. Statistics Poland, 19 December 2024. [Online] Available at: https://stat.gov.pl/en/topics/environment-energy/energy/consumption-of-fuels-and-energy-carriers-in-2023,8,19.html [Accessed 03.01.2025].

Statnett, [n.d.]. NordLink. New subsea interconnector between Norway and Germany. Statnett. [Online] Available at: https://www.statnett.no/en/our-projects/interconnectors/nordlink/ [Accessed 03.01.2025].

Stognei, A., 2024. Russia's shadow fleet grows despite western crackdown. Financial Times. [Online] Available at: https://www.ft.com/content/fbad4462-5ed8-4f75-80d7-79459607277c [Accessed 09.01.2025].

Stuart, L., 2024. Russia's 2023 oil and gas revenues falls to three-year low. S&P Global. [Online] Available at: https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/011124-russias-2023-oil-and-gas-revenues-falls-to-three-year-low [Accessed 09.01.2025].

Svenska Kraftnätt, 2024. Elstatistik. Svenska Kraftnätt, 19 February 2024. [Online] Available at: https://www.svk.se/om-kraftsystemet/kraftsystemdata/elstatistik/ [Accessed 03.01.2025].

Swinhoe, D., 2022. The cable ship capacity crunch. DCD, 6 December 2022. [Online] Available at: https://www.datacenterdynamics.com/en/analysis/the-cable-ship-capacity-crunch/ [Accessed 19.03.2024].

Tammepuu, K., 2023. Ka kõige kallim kaitseplaan ei välista Balticconnectori lõhkumist. Postimees, 18 October 2023. [Online] Available at: https://www.postimees.ee/7878270/ka-koige-kallim-kaitseplaan-ei-valista-balticconnectori-lohkumist [Accessed 19.03.2024].

Tanner, J., 2023. Finnish president says undersea gas and telecom cables damaged by 'external activity'. AP News, 10 October 2023. [Online] Available at: https://apnews.com/article/finland-estonia-pipeline-24d6623cf2778464fdb4ef1d85c70d91 [Accessed 20.02.2024].

Tasavallan Presidentti, 2025. Joint Statement of the Baltic Sea NATO Allies Summit, 14 January 2025. [Online] Available at: https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/ [Accessed 14.01.2025].

TeleGeography, 2024. Submarine Cable Map. Baltic Sea Submarine Cable. [Online] Available at: https://www.submarinecablemap.com/submarine-cable/baltic-sea-submarine-cable [Accessed 19.03.2024].

Ten Houten, M., 2023. Russian spy ships: Mapping undersea infrastructure for sabotage? Digital, 19th of April 2023. [Online] Available at: https://innovationorigins.com/en/russian-spy-ships-mapping-undersea-infrastructure-for-sabotage/ [Accessed 29.02.2024].

Tooming, M., 2023. Auvere jaam hakkab küll taas tööle, kuid elektri hinda see alla ei vii. (26 October 2023). [Online] Available at: https://www.err.ee/1609145063/auvere-jaam-hakkab-kull-taas-toole-kuid-elektri-hinda-see-alla-ei-vii [Accessed 10.07.2024].

Trakimavičius, L., 2021. The Hidden Threat to Baltic Undersea Power Cables. NATO Energy Security Centre of Excellence. [Online] Available at: https://www.enseccoe.org/publications/the-hidden-threat-to-baltic-undersea-power-cables/ [Accessed 01.03.2024].

UNCLOS, 2005. Ühinenud Rahvaste Organisatsiooni mereõiguse konventsioon. RT II 2005, 16, 48. [Online] Available at: https://www.riigiteataja.ee/akt/911675 [Accessed 29.02.2024].

U.S. Army Asymmetric Warfare Group, 2015. Ambiguous Threats and External Influences in the Baltic States. Phase 2: Assessing the Threat. [Online] Available at: https://info.publicintelligence.net/AOWG-ThreatsBalticStates.pdf [Accessed 01.03.2024].

Vabariigi Valitsus, 2024. Michal: Riikidel peab olema võimalus paremini kaitsta oma kriitilist taristut. Valitsuse kommunikatsioonibüroo, 26 December 2024. [Online] Available at: https://www.valitsus.ee/uudised/michal-riikidel-peab-olema-voimalus-paremini-kaitsta-oma-kriitilist-taristut [Accessed 02.01.2025].

Välisluureamet, 2024. Eesti rahvusvahelises julgeolekukeskkonnas 2024. [Online] Available at: https://valisluureamet.ee/doc/raport/2024-et.pdf [Accessed 07.04.2024].

Veebel, V., 2019. Why it would be strategically rational for Russia to escalate in Kaliningrad and the Suwalki corridor. Comparative Strategy, 38(3), pp. 182–197. https://doi.org/10.1080/01495933.2019.1606659.

Vilnius Summit Communiqué, 2023. Vastu võetud NATO riigi- ja valitsusjuhtide poolt, kes osalevad Põhja-Atlandi Nõukogu kohtumisel Vilniuses 11. juulil 2023. [Online] Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm [Accessed 19.03.2024].

Wall, C. & Morcos, P., 2021. Invisible and Vital: Undersea Cables and Transatlantic Security. Center for Strategic and International Studies CSIS. [Online] Available at: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security [Accessed 29.02.2024].

Wasiuta, O., 2023. Russian threats to the submarine internet cable infrastructure. Zeszyty Naukowe SGSP 87:357-378. DOI: 10.5604/01.3001.0053.9127 [Accessed 01.03.2024]. Yle, 2024. Estlink cable disruption: Finnish Border Guard detains tanker linked to Russia's 'dark fleet'. Yleisradio, 26 December 2024. [Online] Available at: https://yle.fi/a/74-20133516 [Accessed 02.01.2025].

Żyła, M., 2019. Kaliningrad oblast in the military system of the Russian Federation. Security and Defence Quarterly, 25(3), pp. 99–117. https://doi.org/10.35467/sdq/105636.

IN AN ERA OF ESCALATING GEOPOLITICAL TENSIONS, CRITICAL UNDERSEA CONNECTIONS BETWEEN COUNTRIES HAVE BECOME PRIME TARGETS IN HYBRID HOSTILITIES.

Given that the likelihood of deliberate attacks on undersea infrastructure has increased in recent years and is expected to remain high in the future, it is essential to plan for accelerated protective measures and implement necessary regulatory adjustments and additional security mechanisms. Assessing potential security threats to Estonia's energy and data infrastructure connecting it to neighboring countries, as well as understanding the risks associated with service disruptions, is therefore critical.

This report examines the growing vulnerabilities of undersea energy and communication links in recent years and outlines necessary risk mitigation measures to ensure better preparedness for probable future threats.

sisekaitse.ee

ISBN 978-9985-67-513-7