Journal on Baltic Security, 2024; 10(2): 1-25

Research Article

Open Access
https://doi.org/10. 10.57767/jobs_2024_008

Ramon Loik*

Undersea Hybrid Threats in Strategic Competition: The Emerging Domain of NATO–EU Defense Cooperation

Received: 27 June 2024.
Accepted: 11 October 2024.

Abstract: This article explains the importance of the underwater critical infrastructure as a domain of hybrid warfare operations and the setting for increasing strategic competition. In addition, the article highlights the growing need for NATO and European Union (EU) defense cooperation in this area, particularly to respond to the strategic ambitions of the Russian Federation and its strategic partnership with China as revisionist powers. Taking a pragmatic case study approach, the article evaluates Russia's current maritime doctrine and characteristic cases of undersea hybrid tactics with several operational examples of Russia's undersea sabotage capabilities. This leads to outlining the emerging NATO–EU inter-organizational defense cooperation in protecting undersea infrastructure. The article concludes with policy advice that the Baltic states, as small open-to-sea member states, should take an active interest in the capability development of the undersea infrastructure protection in both NATO and EU formats.

Keywords: Hybrid threats, undersea infrastructure, defense cooperation, Russia, NATO, European Union

* **Corresponding author:** Ramon Loik, e--mail: ramon.loik@sisekaitse.ee, Analyst of Hybrid Threats at the Internal Security Institute of the Estonian Academy of Security Sciences.

Introduction

The rising importance of undersea infrastructure has made it a prime focus of the escalating great power competition (Runde *et al.*, 2024, p. 10), which, in turn, has raised the need for cooperation between Western countries to protect their critical infrastructure more effectively. Cooperation to strengthen critical infrastructure has become an even more important domain after the sabotage of the Nord Stream pipelines on 26 September 2022 and in response to Russia's 'weaponisation' of energy as part of a war of aggression against Ukraine. NATO's military officials have previously warned that Russia has the technical skills to sabotage some of the world's undersea infrastructure to damage Western digital networks (see, Scott, 2022; Pillai, 2023; Bryant, 2024). One threat scenario circulating in NATO is that the submarines of the Russian Federation may create a readiness to cut submarine cables in the Atlantic Ocean, as well as harm undersea pipelines in other international waters. Since more than 90 percent of the communication between the United States and Europe passes through undersea cables, the consequences of their destruction or damage can be serious. According to Brzozowski (2020) and several other sources (see, among others, Lott, 2022; Nakamura, 2023; Stensrud and Østhagen, 2024), these types of attacks can also be part of hybrid warfare, with operations targeting critical vulnerabilities of a strategic competitor in the 'grey areas' of international waters.

The 2024 Annual Threat Assessment of the US Intelligence Community also emphasises that 'Russia maintains its ability to target critical infrastructure, including undersea cables and industrial control systems, in the United States, as also in allied and partner countries' (Annual Threat Assessment, 2024, p. 16). It is also important to emphasise the dangers of cyber-attacks exploiting the undersea infrastructure (see, Alcaide and Llave, 2020; Bueger and Liebetrau, 2023). By hacking into the network control systems that private companies use to manage data traffic over cables, cyberattackers can significantly disrupt data flows. According to Wall and Morcos (2021), the worst-case scenario would be that a hacker acquires control or administrator rights of the network management system, which allows for discovering physical vulnerabilities in the systems, disrupting or redirecting data traffic, or activating so-called 'kill switch' that deletes the parameters used for data

transmission. Thus, the protection of critical infrastructure in undersea environments is a very complex, multi-domain cooperative task, both politically and technologically.

NATO and the European Union (EU) intensified cooperation in the field of critical infrastructure protection after Russia launched its full-scale war of aggression against Ukraine on 24 February 2022. The sabotage act against the Nord Stream gas pipelines (26 September 2022) and the destruction of the Balticconnector between Finland and Estonia (8 October 2023) were important trigger events pushing this inter-organisational cooperation. At the same time as the latter, undersea communication cables between Estonia and Finland and Estonia and Sweden were also damaged. After these incidents, the NATO Secretary General underlined that these sabotage incidents confirm that undersea infrastructure is vulnerable and that threats to it are real and developing (NATO, 2023c). Since these incidents, NATO has stepped up air and naval patrols and increased its presence in the Baltic and North Seas within the framework of the Joint Expeditionary Force (JEF), led by the United Kingdom (UK).[1] Therefore, Western countries need to recognise the vulnerabilities of their critical infrastructure in the undersea environment and enhance their cooperation to prevent hostile activities by strategic competitors.

The article is divided into four sections. The first section opens the wider international security policy scene on undersea infrastructure as an arena for strategic competition and a domain of hybrid warfare tactics. Second, Russia's current maritime doctrine and some characteristic cases of undersea hybrid tactics are presented. Several operational case examples of Russia's undersea sabotage capabilities and options are described in the following section. Based on that knowledge, some noticeable aspects of NATO–EU emerging inter-organisational cooperation in the protection of undersea critical infrastructure are underlined as a comparative response to Russia's revisionist maritime doctrine and its escalating strategic competition with the West. Methodologically, the pragmatic case study

[1] The Joint Expeditionary Force (JEF) is a UK-led Northern European military partnership for rapid response operations. In addition to the UK, the JEF involves Netherlands, Denmark, Finland, Sweden, Norway, Iceland, Estonia, Latvia and Lithuania.

approach (see, Bueger and Edmunds, 2021) has been chosen to assess actor-practices of hybrid hostilities with revisionist-strategic considerations. A practical defense policy initiative advice for the Baltic states as maritime-open and vulnerable small NATO member states is reasoned in the conclusions.

1. Undersea Infrastructure as a Domain of Strategic and Revisionist Competition

Disruptions to critical infrastructure can seriously affect economic activity, social welfare, or national security (Pillai, 2023, p. 1). Sabotage of critical infrastructure, including undersea infrastructure, can have several conceivable applications, including strategic objectives: for example, the disruption of government communications or national defense control systems in the early stages of a conflict, preventing access to the Internet, harming an economic competitor, or causing supply disruptions, including for geopolitical purposes. A combination of the listed and other tactics can also be used simultaneously (Wall and Morcos, 2021; Fridbertsson, 2023, p. 3) and combined with different attack vectors such as cyberattacks (Guilfoyle *et al.*, 2022), which may be part of wider hybrid hostilities 'designed' to target vulnerabilities, the potential impact of which can be extensive. For example, the UK Ministry of Defense estimates that approximately 99 percent of global Internet traffic operates through undersea cables, and 77 percent of all UK gas imports come from Norway via pipelines under the North Sea (see, Brooke-Holland, 2023). Many NATO and European Union member states with coastlines bordering seas or oceans share similar dependencies on undersea infrastructure, resulting in vulnerabilities.

A more complex operation than damaging or destroying submarine cables is the so-called tapping of them to record, copy, and steal communication data, which can later be analysed for espionage and used for strategic purposes. The latter can be conducted mainly in three ways: inserting 'backdoors' during infrastructure manufacturing, targeting shore-based communication stations and facilities that connect cables to onshore networks, or tapping cables at sea (Wall and Morcos, 2021). Such data espionage is not a new phenomenon in the intelligence activities of great powers. For example, during the Cold War in the 1980s, US intelligence monitored the submarine cable of the Soviet Union as part of Operation 'Ivy Bells',

which provided valuable additional information about the activities, processes, and technologies used by the Soviet fleet (Gehringer, 2023, p. 3). Thus, in the so-called undersea strategic competition, there is a continuous technological arms race and the establishment of positions to advance one's strategic interests.

Since the constant surveillance of the undersea infrastructure is physically and technically complex and very resource-intensive, it is a potentially attractive target for an attacker, the cascading effects of which can have long-term consequences. Locating and fixing damage in subsea infrastructure can be very time-consuming and expensive. An important aspect that adds to the motivation of conducting hybrid operations of undersea infrastructure sabotage is its location in a significant part of the so-called 'grey area'. This is primarily for geographical and legal reasons. More specifically, most of the undersea infrastructure is privately owned or in shared ownership, passes through the jurisdictions of different countries, or is completely outside the jurisdictions of any countries, and their locations are quite well known (Muuga *et al.*, 2024, pp. 43-44). The limiting factor for conducting undersea sabotage operations is their technical complexity and high cost. By rational calculation, the strategic benefits of such operations should be greater than the resources required and the risks taken concerning possible responses. The above leaves little room for random actors in this area of strategic competition and directs attention to technologically capable and motivated state actors and their optional proxies.

Many research sources emphasise the high activity of Russia and China in spying on undersea infrastructure and developing sabotage capabilities, including as an important part of their economic and geostrategic competition with the United States and the EU (see, among others, Burdette, 2021; Bueger *et al.*, 2022; Gehringer, 2023; Insikt Group, 2023; Kaushal, 2023; Kumar, 2023; Nakamura, 2023; Scott, 2022; Siebold, 2023; Ten Houten, 2023). Several sources (see, among others, Roy, 2018; CCDCOE, 2019; Geri, 2023; Long, 2023) highlight the ambition of countries in strategic competition to achieve an informational advantage (preferably dominance) and better cyber-attack positions concerning their rivals through the undersea communication infrastructure. From the broader perspective of

international relations, the Russian Federation and the People's Republic of China can be considered revisionist countries that challenge an undesirable status quo and try to change the structure and balance of power of the international system in their favor by various means (see, among others, Götz and Merlen, 2019; Stent, 2020; Groitl, 2023; Pisciotta, 2023; Saar *et al.*, 2024). While Russia argues from its defense needs position, it promotes a belligerent revisionist strategy in line with its hegemonic strategic goals (Charalambides, 2022, p. 153). Pisciotta (2023, p. 110) explains that Russia and China characterise two types of revisionism. More specifically, Russia represents a nationalist form of revisionism by using military power to control lost territories, counterbalance the US and EU influence in the post-Soviet space, and recover its international position as a great power.

According to Pisciotta (2023), China is a case of reformist revisionism based on a strategy, which tries to increase its power on a global scale mainly by economic and diplomatic means. As a good example of the intensification of economic and geostrategic competition, Gehringer (2023) gives the latest project of the People's Republic of China, 'PEACE' (Pakistan East Africa Connecting Europe), which is part of the 'Digital Silk Road'. With the 15,000-kilometer submarine cable, Pakistan is now connected to Western Europe through the Horn of Africa, the Red Sea, and the Suez Canal. The landing point of the cable is the French coastal city of Marseille. At the same time, the connection with East Africa (through Somalia to Kenya) is also being built. It is also worth noting the fact that the Chinese company Hengtong Optic Electric is one of the largest manufacturers of fiberglass in the world. Russia has currently minimal reliance on undersea infrastructure for its global data transmission. It is connected to the international undersea network through only four cables – one to Finland and Georgia, and two to Japan.

According to Gehringer (2023, p. 5), the limited number of interconnections enables Russia to effectively manage control over the landing points and data traffic of its infrastructure. At the same time, the Russian fleet and various Russian-related vessels have been active in the vicinity of the critical infrastructure of Norway, the United Kingdom, the Netherlands, Belgium, and other NATO and EU member states in the North Sea and the Baltic Sea (see, for example, Page, 2023; Pillai, 2023, p. 5), which indicates their increased interest in intelligence and preparatory activities for possible acts of sabotage. It is important to note increasing strategic

cooperation between Russia and China, which is also evidenced by their joint naval exercises such as 'Ocean–2024' conducted in September 2024 from the Mediterranean to the Pacific (see, Soldatkin and Antonov, 2024; AFP, 2024). In the maritime domain, the intensifying strategic partnership between Russia and China adds a potentially global dimension to this cooperation.

2. Russia's Maritime Doctrine and Cases of Undersea Hybrid Tactics

Russia's revisionist geostrategy is targeted in several directions, including toward Europe, the Arctic Region, the Caucasus Region, and the Middle East (Charalambides, 2022, p. 142). Russia's hybrid tactics represent an acute threat to undersea critical infrastructure in Northern Europe (Monaghan *et al.*, 2023, p. 2), the Atlantic Ocean, the Black Sea, and elsewhere. The war in Ukraine is likely to tie up its conventional forces for some more years, hence, Russia is looking to gain asymmetric advantages in the strategically important area of undersea infrastructure (Muuga *et al.*, 2024, p. 43). The undersea domain is an integral part of both Russian maritime doctrine and the structure of military and intelligence naval operations (Hendriks and Halem, 2024, p. 7, 10, 26). A significant increase in the activity of the Russian Federation fleet in the vicinity of undersea communication cables was observed after the annexation of Crimea in 2014, followed by the expansion of the invasion into eastern Ukraine and the intervention in the Syrian civil war in 2015 (Sanger and Schmitt, 2015). Therefore, member states of NATO and the European Union should improve information sharing and develop comprehensive monitoring and defense strategies in this domain.

More specifically, Section 15 of the Maritime Doctrine of the Russian Federation (2022) defines (1) the waters of the oceans and seas adjacent to the littorals of the Russian Federation, including the Sea of Azov and the Black Sea; (2) the eastern part of the Mediterranean Sea; (3) the Black Sea, Baltic, and Kuril Straits, and (4) areas of the world's maritime transport lines of communication, including those along the Asian and African coasts, as important areas (zones) for 'ensuring the national interests and maintaining the strategic and regional security of the Russian Federation'. Section 20 of the same doctrine reasons these national strategic security

interests by stating the following: 'The Russian Federation's independent foreign and domestic policy is opposed by the United States and its allies, who seek to maintain their dominance in the world, including in the World Ocean. They have implemented a policy of containment of the Russian Federation, which includes political, economic, military, and informational pressure against the state'.[2] It can be observed that the doctrine is formulated apparently as 'defensive', but the below examples of the activities of the Russian fleet confirm active disruption operations and the creation of possible offensive positions against the critical undersea infrastructure of several NATO countries.

Defining the position of strategic competition in the doctrine continues by Section 53 (*ibid.*), which emphasises that 'The national maritime policy in the Atlantic regional area is determined by the existence of NATO, which focuses its activities on confrontation with the Russian Federation and its allies', and is further developed in Section 54 by declaring that 'The decisive factor in relations with NATO continues to be the plans of the Alliance to advance its military infrastructure to Russia's borders and its attempt to globalise its operations, which is unacceptable for the Russian Federation'. Section 105 of the Maritime Doctrine of the Russian Federation (2022) emphasises that the 'Russian Federation will resolutely and decisively defend its national interests in the World Ocean, and the availability of sufficient maritime power guarantees its security and protection'. The foregoing expresses the Russian Federation's political-strategic will as well as its doctrinal mission statement for hybrid activities in the global maritime domain, wherever Russia sees its own economic or security interests at stake. The active revisionist and power-competitive nature of the doctrine is openly characterised by statements from President Putin on the joint exercise of the fleets of Russia and China 'Ocean–2024', warning that 'Russia should be ready for any developments and would keep strengthening its naval forces, including their nuclear component, in the face of an arms race driven by Washington' (see, Soldatkin and Antonov, 2024).

There have been several incidents of damage to undersea infrastructure in the Baltic Sea, in which Russia's involvement has either been identified or suspected. For

[2] Unofficial translation of the doctrine by Anna Davis and Ryan Vest from Russia Maritime Studies Institute, United States Naval War College.

example, in the first half of 2015, the Nordbalt cable between Lithuania and Sweden was repeatedly damaged by Russian ships. The mentioned 400-kilometer-long infrastructure runs from Klaipeda to Nybro on the east coast of Sweden and increases the security of electricity supply in both the Nordic countries and Lithuania. Russia responded to the governments of Sweden and Lithuania at the time that their actions were aimed at protecting the country's 'military exercise zone' (Euractiv, 2015). Generally, an attempt is made to hide this kind of hostilities and to ensure the so-called plausible deniability for a possible attacker, leaving the impression of some kind of 'accident', using various proxy actors or other conspiratorial ways to mislead the investigation of cases. For the Russian fleet, for example, the regular repair and maintenance works of the Nord Stream pipelines provided a good 'cover' to ensure such plausible deniability as a basis for intelligence and sabotage activities in the Baltic Sea (see, Ryzhenko, 2022).

Another remarkable incident occurred on 7 January 2022, when the undersea fiber-optic cable between mainland Norway and the Svalbard archipelago in the Arctic Ocean was offline, actually being cut after Russian fishing vessels had been observed in the area (see, Stensrud and Østhagen, 2024, pp. 117–118). The military value of the cable, as well as the Svalbard Satellite Station (SvalSat), suggest possible motivations for some espionage or sabotage missions. Despite Svalbard being a designated demilitarised zone, there have been suggestions, including from Russia, that the SvalSat facilities are used to download data from military and commercial satellites. Furthermore, the cables are part of a vital passageway for Russian naval vessels, including surface ships and submarines, to proceed from their bases into the Atlantic. According to Ryzhenko (2022), the incident's location in the increasingly strategic Arctic region adds to the suspicion that Russian operatives could be involved. In the next section, some further detailed case examples of Russia's undersea sabotage capabilities will be presented.

3. Case Examples of Russia's Undersea Sabotage Capabilities

Russia has shown increased interest in transatlantic undersea cables in recent years, especially in the North Atlantic Ocean. This coincides with NATO's growing

awareness of the importance and vulnerability of these undersea cables. Since Russia relies significantly less on undersea communications than the United States or China, it is less vulnerable to disruptions in subsea cable infrastructure and potentially more motivated to exploit these vulnerabilities in other countries. As proof of this, following the explosions on the Nord Stream pipeline in 2023, high-ranking Russian officials, such as Dmitry Medvedev, the deputy chairman of Russia's Security Council, have emphasised the perspective that Russia could retaliate against alleged Western involvement in the blasts by targeting their undersea communication cables (Runde *et al.*, 2024, p. 5; see also Faulconbridge, 2023). Evaluating such rhetoric from the political leadership in conjunction with Russia's maritime doctrine explained above and with some action examples below, one can assume that the threat can be considered serious.

The Main Directorate of Deep-Sea Research (in Russian: *Главное управление глубоководных исследований* – GUGI) under the Ministry of Defense of the Russian Federation is known to use spy ships, specialised submarines, and the ability to deploy aquanauts, mini submarines, or underwater drones. In 2018, some 17 underwater drone projects were known to be in operation in Russia. Possible attack methods include detonating torpedo warheads or laying remote-activated mines (Ten Houten, 2023). Although the GUGI operates independently from the other armed forces (as a specialized unit), its ships and personnel are also often associated with various parts of the Russian Navy fleet. For example, Russian naval personnel in the area were reported during the last phase of the Nord Stream 2 construction (from 10 April to 30 August 2021). A joint special operations group was spotted aboard civilian ships of the Russian Maritime Rescue Service. The members of the joint group were assigned to different special units of the Russian Navy (data from Ryzhenko, 2022): four members from GUGI, seven members from the 313th Special Purpose Detachment for Combating Underwater Sabotage of the Baltic Fleet, and seven members of the 342nd Emergency Rescue Detachment of the Baltic Fleet.

One of the suspected GUGI tools is the special purpose vessel for oceanographic research 'Yantar' (in Russian: *Янтарь*), which received closer attention for operating around sensitive undersea cables near the UK in 2019 (see, Kaushal, 2023) and which has been spotted periodically around the world, from the Caribbean to the

Persian Gulf and off the coast of Ireland near the AEC-1 infrastructure and the Celtic-Norwegian submarine cables. As Nakamura (2023) reports, with submersibles capable of operating at a depth of approximately 6,000 meters, the 'Yantar' is suspected of spying on seabed infrastructure and equipment such as submarine cables and underwater sensors. In addition, the Russian Naval Intelligence Directorate also has assets capable of conducting various espionage and sabotage operations under the command of military intelligence, the GRU. Sabotaging and taking control of communication cables has always been an important line of operation for Russian special services. During the 2014 Crimean annexation, Russian invasion forces cut off the main terrestrial cable connection to gain control of the peninsula's Internet infrastructure and spread disinformation (Bueger *et al.*, 2022, p. 32). The latter added an element of surprise to the annexation operation and provided the necessary 'time window' to achieve informational superiority.

According to Wall and Morcos (2021), Russia has two main ways to directly threaten the undersea cables by using submarines or surface vessels capable of deploying autonomous or manned submersibles. For example, the Russian deep-diving nuclear-powered submarine known as 'Losharik' (in Russian: *Лошарик*) was capable of mapping or potentially damaging undersea cables until it was decommissioned due to a fire in 2019. While the 'Losharik' is being repaired, the Russian Navy has other similar submarines, such as the nuclear-powered 'Poseidon', and is also developing unmanned undersea drones. In April 2023, Swedish, Danish, Norwegian, and Finnish broadcasters published a report on a joint investigation of the surveillance of the Russian fleet in the North Sea, including the 'Admiral Vladimirsky' (in Russian: *Адмирал Владимирский*), believed to be a Russian maritime intelligence vessel, which had been sailing near wind farms. The ship was manned by persons wearing face masks and bulletproof vests and equipped with machine guns. The broadcasters involved in the investigation used a variety of data analysis, intercepted radio communications, and various sources of information to prove that approximately 50 vessels had been gathering intelligence in the North Sea region over the past 10 years, using underwater surveillance equipment to map key

locations for potential sabotage (see, Corera, 2023; Fastrup *et al.*, 2023; Hou *et al.*, 2023).

Ryzhenko (2022) reports that in 2021, there were suspicious underwater activities in the maritime economic zones of Denmark and Germany near the fiber-optic communication lines of 'Baltica', which connect Poland, Sweden, and Denmark, and Denmark-Poland 2. These activities occurred within two to three miles of Nord Stream 2. During this time, the Russian rescue vessel 'Bakhtemir' (in Russian: *Бахтемир*) and a group of divers, a mobile deployment diving station, and a remote-controlled submersible were involved in several weeks of underwater activities in the area. The 'Bakhtemir' was equipped with cable cutters, potentially for sabotage operations on the seabed in the shallow Baltic. Similar operations have targeted Norwegian infrastructure. In April 2021, the seabed sensors of the Lofoten-Vesteralen Ocean Observatory (LoVe) on the Norwegian Continental Shelf were deactivated. The system collected scientific data with information about passing submarines and other undersea objects. Reports (*ibid.*) noted that more than 2.5 miles of fiber-optic and electrical cables were severed and then removed, weighing around 9.5 tons in total.

In the case of the previous examples, which is far from complete, it must be recognised that the circumstances are partially unproven, or a version derived by logically connecting fragments of known facts. At the same time, connecting the known dots and comparing different episodes allows us to identify some patterns, such as 'civil' marine research, fishing vessels, or 'maintenance works' near subsea infrastructure facilities as Russian *modus operandi*, and identify the authors of the incidents by comparing them with doctrinal tasks and known resources. Further proof that Russia is investing in the development of undersea monitoring and sabotage capabilities is the recent construction of ice-classed intelligence ships 'Leonid Bekrenev' and 'Boris Bobkov' under Project 03182R (see, Baudu *et al.*, 2023, p. 10; Nilsen, 2023), which strengthens Navy's Intelligence Directorate reach for seafloor operations. These factual examples prove both Russia's active interest and real capabilities to spy on, disturb and, if necessary, damage critical undersea infrastructure.

4. NATO–EU Emerging Cooperation in the Protection of Undersea Critical Infrastructure

Although the need for the protection of undersea infrastructure does not represent a new challenge, increasing dependence on it and the escalation of strategic competition have increasingly raised the need for defense cooperation in this domain of hybrid hostilities. Nakamura (2023) suggests that given the war in Ukraine and the expansion of NATO, transatlantic allies must make a concerted effort to strengthen the defense of their undersea infrastructure against Russian hybrid tactics. Several referenced analyses in this regard already paid attention to the vulnerabilities of the undersea critical infrastructure and the need for enhanced cooperation between NATO and the European Union countries as the Ukrainian conflict has escalated into a full-scale war and also offered some recommendations for the development of such cooperation (see, among others, Gallagher, 2022; Hartmann, 2023; Nakamura, 2023; Pillai, 2023). Specifically highlighted, Wall and Morcos (2021) recommended that the United States and its European allies and partners should work closely with the private sector to develop plans to prepare for the consequences of planned (or unintended) subsea infrastructure disruptions. Special attention must be paid to potential risk scenarios where several connections are broken simultaneously.

Gehringer (2023, p. 3) points out in his analysis that a complete interruption of all data traffic is still currently unrealistic. Damage to one cable will not cause a complete interruption of data transmission, provided that alternative options within the network are available. If individual cable connections are destroyed, the data 'looks' for another viable route through the cable infrastructure, which can cause data communication delays. In this case, the risk of network overload also increases. He adds (*ibid.*) that a simultaneous physical attack on several undersea cables is theoretically possible. Still, in addition to knowing the exact location of the cable route, this would require extensive preparation and a huge number of resources. At the same time, public information about the routes of submarine cables and the locations of landing points adds to the security risks. In any case, it is important to

consider these circumstances in different risk scenarios and preventive measures. The latter is an area where NATO and EU member states should improve coordination of their respective procedures and capacity development, including compensating capacity gaps, both among themselves and within the institutions.

Wall and Morcos (2021) also emphasise that a planning process based on threat scenarios could help governments and infrastructure owners identify national contact points, organise regular exercises, and find ways to improve the resilience of systems. According to them, this could certainly be an important area of coordinative cooperation between the European Union and NATO, which applies the strengths of both organizations, including the EU's financial and regulatory competence and NATO's experience in the field of defense planning. Both organisations have created strategic foundations and institutional networks to enhance cooperation in critical infrastructure protection. A concrete example of that is the EU–NATO Task Force on the Resilience of Critical Infrastructure, which was announced by the Commission President and NATO Secretary General in January 2023 (see, European Commission, 2023, p. 19). This emerging domain of NATO–EU defense cooperation is also interesting from a perspective of academic research, as the 'EU–NATO relationship' has become a 'catalytic case study' in terms of advancing conceptual efforts to theorise complex inter-organisational relations in International Relations (Koops, 2017, p. 315). In addition, as Ewers-Peters (2022) emphasises, the EU and NATO's largely overlapping member states in these organisations are often in competition for their own national security interests and preferences, and this dynamic largely determines the motivation for cooperation and the perspectives of both organisations.

NATO's Strategic Concept, which Heads of State and Government adopted at the NATO Summit in Madrid on 29 June 2022, states in Section 23 that 'Maritime security is key to our peace and prosperity. We [NATO member states] will strengthen our posture and situational awareness to deter and defend against all threats in the maritime domain, uphold freedom of navigation, secure maritime trade routes, and protect our main lines of communications'. Section 8 of the concept stresses that Moscow's military build-up, including in the Baltic-, Black- and Mediterranean Sea regions, challenge our [NATO] security and interests' (North Atlantic Treaty Organization, 2022). At the Vilnius Summit in July 2023,

NATO member states agreed to establish NATO's Maritime Center for the Security of Critical Undersea Infrastructure in the United Kingdom at the NATO Naval Command (MARCOM) and to create a special cooperation network that connects the governments of NATO member states with the private sector and other with the necessary parties to improve communication and develop best practices (see, Vilnius Summit Communiqué, 2023, point 65; Monaghan *et al*., 2023, p. 1). Also important to note is NATO's maritime security operation 'Sea Guardian' (see, United States Navy, 2022), which, among other tasks, focuses on raising situational awareness, fighting terrorism, and developing response capabilities in the Mediterranean region.

The integration of the maritime defense technologies of the member states and the improvement of interoperability must be seen as an important potential for cooperation. Therefore, NATO's Science and Technology Organization (STO) and its Centre for Maritime Research and Experimentation (STO CMRE), based in La Spezia, Italy, is likely to play an increasing role in providing innovative, science and technology-based solutions to address existing maritime capability gaps (Fridbertsson, 2023, pp. 8-9). NATO is rushing to develop technologies that allow real-time detection of suspicious activity near underwater critical infrastructure and is testing maritime drones, various sensors, and the application of artificial intelligence. The latter can be used, among other tools, to track ships when they repeatedly cross critical undersea infrastructure. In future developments, so-called smart fiber-optic cables can also detect interference in their vicinity (Lima and Drozdiak, 2023). Surveillance and protection of subsea infrastructure is technologically complex, expensive, and requires many parties' cooperation, including closer public-private collaboration and data-sharing. According to Hendriks and Halem's (2024, pp. 11-12) report, air-based data and satellite imagery should be integral components of a maritime defense system, as undersea acoustic signals need to be cross-checked with satellite imagery for maximum surveillance and identification precision.

In February 2023, NATO launched a Critical Undersea Infrastructure Coordination Cell at its Headquarters, and at the beginning of the same year, NATO and the

European Union jointly launched a new Task Force on the Resilience of Critical Infrastructure, which focuses on the energy, transport, digital infrastructure, and space sectors (see, NATO, 2023a; 2023b). These cooperation formats are still relatively new and need some time to achieve operational maturity, but they are undoubtedly necessary steps for resource planning and consolidated capability development. As Hendriks and Halem (2024, p. 11) emphasise that new undersea defense cooperation formats between NATO and EU are still 'limited to establishing definitions and formulating strategic concepts'. Also, 'capability development coordination, and regularized joint operations towards clear strategic aims, are needed to create an interconnected defensive system to ward off hostile sub-surface activities' (*ibid.*). The latter is essential from the point of view of small member states, which individually lack both competence and resources for integrated defense solutions.

Among the most recent developments in the European Union aimed at protecting critical undersea infrastructure is the update of the EU Maritime Security Strategy and its action plan in 2023 (see, European Union, 2023), which provides for a series of measures to protect vital marine infrastructure, such as gas pipelines, power and communication cables, ports, offshore energy facilities, LNG terminals, floating storages, and other facilities, and to increase the resilience and protection of marine equipment. Also, measures to improve cyber security and to increase resistance to information manipulation and other hybrid threats related to maritime security are stipulated in the strategy and its implementation plan. In parallel with the update of the EU Maritime Security Strategy, the European Defense Agency (EDA) is developing the Maritime Surveillance Networking Project (MARSUR), which aims to improve member states' maritime comprehensive situation awareness, including hybrid threats (see, European Commission, 2023, p. 9).

In summary, Russia's war of aggression against Ukraine, the rise of the Russia–China strategic and revisionist partnership, and the intensified hybrid hostilities have given a significant impetus to the development of cooperation between the European Union and NATO to a new level, and the protection of critical infrastructure, including the undersea critical infrastructure, is among the priorities

agreed by both organisations, which requires needful care to achieve the necessary cooperation synergy for real capability development.

Conclusion

The current maritime security doctrine of the Russian Federation from 2022 defines the United States, NATO, and their allies as its sharp strategic opponents and provides for Russia's action in the seas 'resolutely and decisively', based on its own security and economic interests. Assessing the several examples presented in the article, it is evident that Russia has the political motivation, doctrinal basis, and significant resources to disrupt and sabotage the critical undersea infrastructure of its 'strategic adversaries' as part of an array of its hybrid warfare tactics. More specifically, sabotage of undersea critical infrastructure can have several conceivable applications, including strategic objectives. For example, disrupting government communications or national defense control systems in the early stages of a conflict, hindering access to the Internet, harming an economic competitor, or causing trade obstructions for geopolitical purposes. A combination of the listed and other tactics can also be used simultaneously, possibly as part of hybrid hostilities designed to target the vulnerabilities of strategic competitors.

According to multiple sources referenced in the article, Russia's hybrid tactics pose an acute threat to critical undersea infrastructure in Northern Europe, the Atlantic Ocean, the Black Sea, and elsewhere. Targeting the critical infrastructure, including undersea infrastructure, is an important line of Russia's military doctrine, and with the war in Ukraine likely to tie up its conventional land forces for some more years, Russia is looking to achieve some asymmetric advantages elsewhere, including in the strategically key area of undersea infrastructure. For this doctrinal purpose, capabilities for spying and sabotaging undersea infrastructure have been created, implemented, and developed both within the Russian Navy and under the cover of various (civil) oceanographic studies. The documented cases of recent years in both the North Sea and the Baltic Sea, discussed in the article, demonstrate that the specialised units of the Russian fleet have activated their mapping and disruptive

activities of the undersea infrastructure of NATO member states to prepare possible subsequent acts of sabotage.

Most of the undersea infrastructure, including critical infrastructure, is privately owned or in shared ownership, passes through the authorities of different countries, or is completely outside the jurisdictions of countries and it is relatively publicly known where they are located. The mentioned circumstances make the complete defence of undersea infrastructure difficult and protective measures very resource-intensive, and thus make undersea infrastructure a potentially vulnerable target, including in the hybrid strategies of hostile actors. This highlights the need to specify the relevant maritime law in the conditions of escalating strategic competition, to reduce 'grey zones', and increase the cooperation of international organisations. According to the referenced experts, full protection of the undersea infrastructure is impossible without closer cooperation between the public and private sectors and the sharing of relevant data. Aerial observation data and satellite imagery are integral components of a subsea infrastructure protection system, as subsea acoustic signals must be cross-checked with satellite data to ensure accurate detection. Therefore, protection solutions for the undersea critical infrastructure need to be developed through international cooperation, including the European Union and NATO, as the small member states such as the Baltic states alone do not have the necessary resources and capabilities.

NATO and the EU intensified cooperation on the protection of critical infrastructure, including undersea infrastructure, after Russia started a full-scale war of aggression against Ukraine on 24 February 2022. The sabotage act against the Nord Stream gas pipelines and the destruction of the Balticconnector between Finland and Estonia raised the challenge even more acutely. Operationally, the UK-lead JEF reacted the fastest to the latter incident. To date, the NATO Maritime Center for the Security of Critical Undersea Infrastructure has also been established in the United Kingdom under the NATO Naval Command (MARCOM), as well as the NATO–European Union Critical Infrastructure Resilience Working Group and other expert-level cooperation formats. Since this field of inter-organisational cooperation is quite new, it will still have to be equipped with specific capabilities in the following years, which could potentially raise NATO-EU cooperation to a

new level, applying the strengths of both organisations as the EU's regulatory competencies and NATO's capabilities in the field of joint defense planning.

As a practical defense policy advice, the Baltic states should take an active interest position in the capability development of undersea infrastructure protection both in NATO and in the European Union formats, because, on the one hand, they are vulnerable in terms of this critical infrastructure domain, on the other hand, independent capability development in this area is very resource-intensive for small member states alone. However, a permanent and sufficiently deterrent solution is necessary. As long as the global strategic competition intensifies in the coming years, Western countries not only have the opportunity but also the existential need to ensure their deterrence and convincing defense capabilities through the enhanced cooperation of NATO and the European Union.

Bibliography

AFP. (2024) 'Russia launches largest navy drills of post-Soviet era alongside China in Sea of Japan', *France24* [Online] 10 September 2024. https://www.france24.com/en/live-news/20240910-russia-china-join-forces-for-major-naval-exercise (Accessed: 11 September 2024).

Alcaide, Juan Ignacio and Llave, Ruth Garcia. (2020) 'Critical infrastructures cybersecurity and the maritime sector', *Transportation Research Procedia*, Vol. 45, pp. 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.

Annual Threat Assessment. (2024) *Annual Threat Assessment of the U.S. Intelligence Community*. Office of the Director of National Intelligence [Online] 5 February 2024. https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (Accessed: 20 March 2024).

Baudu, Hervé; Canova, Émilie; Delaunay, Michael; Escude-Joffres, Camille; Sandre, Tanguy; Taithe, Alexandre; Tasse, Julia; Thevenoux, Pierre; Vanderlinden, Jean-Paul; Vidal, Florian and Vullierme, Magali. (2023) 'Observatoire de l'Arctique', *Bulletin No. 40*. Fondation pour la Recherche Stratégique. [Online] May 2023. https://www.defense.gouv.fr/sites/default/files/dgris/ObsArctique_Bulletin4_Mai_2023.pdf (Accessed: 30 September 2024).

Brooke-Holland, Louisa. (2023) *Seabed warfare: Protecting the UK's undersea infrastructure*. House of Commons Library. [Online] 24 May 2023. https://commonslibrary.parliament.uk/seabed-warfare-protecting-the-uks-undersea-infrastructure/ (Accessed: 29 February 2024).

Brzozowski, Alexandra. (2020) 'NATO seeks ways of protecting undersea cables from Russian attacks', *Euractiv*. [Online] 23 October 2020. https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/ (Accessed: 29 February 2024).

Bryant, Miranda. (2024) 'Undersea "hybrid warfare" threatens security of 1bn, NATO commander warns', *The Guardian*. [Online] 16 April 2024. https://www.theguardian.com/world/2024/apr/16/undersea-hybrid-warfare-threatens-security-of-1bn-nato-commander-warns (Accessed: 2 September 2024).

Bueger, Christian and Edmunds, Timothy. (2021) 'Pragmatic ordering: Informality, experimentation, and the maritime security agenda', *Review of International Studies*, Vol. 47(2), pp. 171–191. https://doi.org/10.1017/S0260210520000479.

Bueger, Christian and Liebetrau, Tobias. (2023) 'Critical maritime infrastructure protection: What's the trouble?', *Marine Policy*, Vol. 155. Article 105772. https://doi.org/10.1016/j.marpol.2023.105772.

Bueger, Christian; Liebetrau, Tobias and Franken, Jonas. (2022) *Security threats to undersea communications cables and infrastructure – consequences for the EU*. European Parliament. [Online] June 2022. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf (Accessed: 29 February 2024).

Burdette, Lane. (2021) 'Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy', *Journal of Public and International Affairs*. [Online] 5 May 2021. https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy (Accessed: 29 March 2024).

CCDCOE. (2019) 'The strategic importance of, and dependence on, undersea cables', *NATO Cooperative Cyber Defence Centre of Excellence CCDCOE*. [Online] November 2019. https://www.ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf (Accessed: 29 February 2024).

Charalambides, Yiannos. (2022) 'A Russian Revisionist Strategy on the Rise?', *Strategic Analysis*, Vol. 46(2), pp. 141–156. https://doi.org/10.1080/09700161.2022.2076303

Corera, Gordon. (2023) 'Ukraine war: The Russian ships accused of North Sea sabotage', *BBC News* [Online] 19 April 2023. https://www.bbc.com/news/world-europe-65309687 (Accessed: 25 March 2024).

Euractiv. (2015) 'Russia accused of disrupting new energy link between Sweden and Lithuania', *Euractiv Media Network BV* [Online] 4 May 2015. https://www.euractiv.com/section/global-europe/news/russia-accused-of-disrupting-new-energy-link-between-sweden-and-lithuania/ (Accessed: 20 March 2024).

European Commission. (2023) *Seventh progress report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*. 15.09.2023, SWD(2023) 315 final. Brussels. [Online] 25 September 2023. https://data.consilium.europa.eu/doc/document/ST-13344-2023-INIT/en/ (Accessed: 12 September 2024).

European Union. (2023) *Joint Communication to the European Parliament and the Council on the update of the EU Maritime Security Strategy and its Action Plan "An enhanced EU Maritime Security Strategy for evolving maritime threats"*. 10.03.2023, JOIN(2023) 8 final. Brussels. [Online] 10 March 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0008 (Accessed: 25 March 2024).

Ewers-Peters, Nele Marianne. (2022) *Understanding EU-NATO Cooperation: How Member-States Matter* (1st ed.). London: Routledge. https://doi.org/10.4324/9781003170068.

Fastrup, Niels; Quass, Lisbeth and Thim, Frederik Hugo Ledegaard. (2023) 'Afsløring: Russiske spionskibe forbereder mulig sabotage mod havvindmøller, gasrør og strømkabler i Danmark og Norden' [Disclosure: Russian spy ships are preparing possible sabotage against offshore wind turbines, gas pipes and power cables in Denmark and the Nordics], *DR* [Online] 19 April 2023. https://www.dr.dk/nyheder/indland/moerklagt/afsloering-russiske-spionskibe-forbereder-mulig-sabotage-mod (Accessed: 26 March 2024).

Faulconbridge, Guy. (2023) 'Russia now has free hand to destroy undersea communications cables, Putin ally says', *Reuters* [Online] 14 June 2023. https://www.reuters.com/world/europe/russias-medvedev-says-moscow-now-has-free-hand-destroy-enemies-undersea-2023-06-14/ (Accessed: 23 September 2024).

Fridbertsson, Njall Trausti. (2023) *Protecting Critical Maritime Infrastructure – The Role of Technology*. General Report. 032 STC 23 E. NATO Parliamentary Assembly: Science and Technology Committee (STC). [Online] 2023. https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc (Accessed: 21 March 2024).

Gallagher, Jill. (2022) *Undersea Telecommunication Cables: Technology Overview and Issues for Congress*. Congressional Research Service. [Online] 2022. https://crsreports.congress.gov/product/pdf/R/R47237 (Accessed: 29 March 2024).

Gehringer, Ferdinand Alexander. (2023) 'Undersea cables as critical infrastructure and geopolitical power tool', *Facts and Findings, No. 495*. Konrad-Adenauer-Stiftung. [Online] https://www.kas.de/documents/252038/22161843/Undersea+cables.pdf/aee8e59b-96dc-bc05-18ac-b1070eb76bc1 (Accessed: 29 March 2024).

Geri, Maurizio. (2023) 'South China Sea tensions conceal a secret war to control the world's Internet', *Euractiv* [Online] 2 May 2023. https://www.euractiv.com/section/china/opinion/south-china-sea-tensions-conceal-a-secret-war-to-control-the-worlds-internet/ (Accessed: 29 March 2024).

Groitl, Gerlinde. (2023) *Russia, China and the Revisionist Assault on the Western Liberal International Order*. Palgrave Macmillan.

Guilfoyle, Douglas; Paige, Tamsin Phillipa and McLaughlin, Rob. (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.

Götz, Elias and Merlen, Camille-Renaud. (2019) 'Russia and the question of world order', *European Politics and Society*, Vol. 20(2), pp. 133–153. https://doi.org/10.1080/23745118.2018.1545181.

Hartmann, Jannik. (2023) 'Protecting the EU's Submarine Cable Infrastructure: Germany's Opportunity to Transform Vulnerability into Mutual Resilience', *German Council on Foreign Relations DGAP*. [Online] 10 June 2023. https://dgap.org/en/research/publications/protecting-eus-submarine-cable-infrastructure (Accessed: 29 March 2024).

Hendriks, Marcus Solarz and Halem, Harry. (2024) 'From space to seabed: Protecting the UK's undersea cables from hostile actors', *Policy Exchange* [Online] 2024. https://policyexchange.org.uk/wp-content/uploads/From-space-to-seabed.pdf (Accessed: 19 March 2024).

Hou, Li-Lian Ahlskog; Goodwin, Allegra; Chernova, Anna and Cotovio, Vasco. (2023) 'Fleet of Russian spy ships has been gathering intelligence in Nordic waters, investigation finds', *CNN* [Online] 20 April 2023. https://edition.cnn.com/2023/04/19/europe/russia-spy-ships-nordic-waters-intl/index.html (Accessed: 25 March 2024).

Insikt Group. (2023) 'The Escalating Global Risk Environment for Submarine Cables', *Recorded Future*. [Online] 27 June 2023. https://www.recordedfuture.com/escalating-global-risk-environment-submarine-cables (Accessed: 28 February 2024).

Kaushal, Sidharth. (2023) 'Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure', *The Royal United Services Institute for Defence and Security RUSI*. [Online] 25 May 2023. https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure (Accessed: 28 February 2024).

Koops, Joachim Alexander. (2017) 'Theorising inter-organisational relations: the "EU–NATO relationship" as a catalytic case study. *European Security*, Vol. 26(3), pp. 315–339. http://dx.doi.org/10.1080/09662839.2017.1352583

Kumar, Raghvendra. (2023) 'Securing the Digital Seabed: Countering China's Underwater Ambitions', *Journal of Indo-Pacific Affairs*, November-December 2023. pp. 74–90.

Lima, Joao and Drozdiak, Natalia. (2023) 'NATO Turns to Underwater Drones and AI in Bid to Deter Russia', *Bloomberg News*. [Online] 28 September 2023. https://news.bloomberglaw.com/artificial-intelligence/nato-turns-to-underwater-drones-and-ai-in-bid-to-deter-russia (Accessed: 28 February 2024).

Long, Madison 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] May 2023. https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks (Accessed: 28 February 2024).

Lott, Alexander. (2022) 'Hybrid Threats and the Law of the Sea', *International Straits of the World Series*, Vol. 19. Brill Nijhoff. https://doi.org/10.1163/9789004509368.

Maritime Doctrine of the Russian Federation. (2022) Approved by the Decree of the President of the Russian Federation on 31 July 2022 No. 512. Moscow, Kremlin.

Monaghan, Sean; Svendsen, Otto; Darrah, Michael and Arnold, Ed. (2023) 'NATO's Role in Protecting Critical Undersea Infrastructure', *Center for Strategic and International Studies CSIS*. [Online] 19

December 2023. https://www.csis.org/analysis/natos-role-protecting-critical-undersea-infrastructure (Accessed: 28 February 2024).

Muuga, Emilia; Loik, Ramon; Kaup, Georg-Henri; Savimaa, Raul; Koort, Erkki. (2024) *Julgeolekuohud Balti riikide merealuste ühendustega seotud kriitilisele taristule* [Security Threats to the Undersea Connections Related Critical Infrastructure of the Baltic States]. Tallinn: Sisekaitseakadeemia (Estonian Academy of Security Sciences). https://doi.org/10.15158/6akf-fm57.

Nakamura, Hotaka. (2023) 'The Enemy Below: Fighting against Russia's Hybrid Underwater Warfare', *Center for Maritime Strategy*. [Online] 29 June 2023. https://centerformaritimestrategy.org/publications/the-enemy-below-fighting-against-russias-hybrid-underwater-warfare/ (Accessed: 28 February 2024).

NATO. (2023a) *NATO and the EU set up a taskforce on resilience and critical infrastructure.* [Online] 11 January 2023. https://www.nato.int/cps/en/natohq/news_210611.htm (Accessed: 28 February 2024).

NATO. (2023b) *NATO and European Union launch task force on resilience of critical infrastructure.* [Online] 16 March 2023. https://www.nato.int/cps/en/natohq/news_212874.htm (Accessed: 19 March 2024).

NATO. (2023c) *NATO Secretary General addresses protection of critical undersea infrastructure, support to Ukraine with EU Defence Ministers*. [Online] 14 November 2023. https://www.nato.int/cps/en/natohq/news_220058.htm (Accessed: 28 February 2024).

Nilsen, Thomas. (2023) 'Navy's Intelligence Directorate gets four more ice-classed spy ships for seafloor operations', *The Barents Observer*. [Online] 25 April 2023. https://www.thebarentsobserver.com/security/navys-intelligence-directorate-gets-four-more-iceclassed-spy-ships-for-seafloor-operations/162832 (Accessed: 30 September 2024).

North Atlantic Treaty Organization. (2022) *NATO 2022 Strategic Concept*, Adopted by Heads of State and Government at the NATO Summit in Madrid on 29 June 2022. [Online] 2022. https://www.nato.int/strategic-concept/ (Accessed: 25 June 2024).

Page, Mercedes. (2023) 'Russia, a Chinese cargo ship and the sabotage of subsea cables in the Baltic Sea', *The Strategist*. [Online] 31 October 2023. https://www.aspistrategist.org.au/russia-a-chinese-cargo-ship-and-the-sabotage-of-subsea-cables-in-the-baltic-sea/ (Accessed: 28 February 2024).

Pillai, Helmi. (2023) 'Protecting Europe's critical infrastructure from Russian hybrid threats', *Centre for European Reform*. [Online] 25 April 2023. https://www.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid (Accessed: 28 February 2024).

Pisciotta, Barbara. (2023) 'Regional and Global Revisionism: Russia and China in a Comparative Perspective', *The International Spectator*, Vol. 58(3), pp. 96–112. https://doi.org/10.1080/03932729.2023.2194161.

Roy, Saurav. (2018) 'Protecting Undersea Cables: An Underrated Element of International Cybersecurity', *Cambridge International Law Journal*. [Online] https://cilj.co.uk/2018/02/02/protecting-undersea-cables-an-underrated-element-of-international-cybersecurity/ (Accessed: 28 February 2024).

Runde, Daniel F.; Murphy, Erin L. and Bryja, Thomas. (2024) 'Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition', *Center for Strategic and International Studies CSIS*. [Online] 16 August 2024. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition (Accessed: 23 September 2024).

Ryzhenko, Andrii. (2022) 'Nord Stream Explosions: Russian Sabotage in the Baltic?', *Eurasia Daily Monitor,* 19(146). The Jamestown Foundation. [Online] 4 October 2022. https://jamestown.org/program/nord-stream-explosions-russian-sabotage-in-the-baltic/ (Accessed: 23 March 2024).

Saar, Jüri; Sinisalu, Arnold; Loik, Ramon; Koort, Erkki; Tammel, Kaide and Savimaa, Raul. (2024) *Venemaa võimalike arengute mõjust Eesti julgeolekule* [The Impact of Russia's Alternative Future Developments on Estonian Security]. Tallinn: Sisekaitseakadeemia (Estonian Academy of Security Sciences). https://doi.org/10.15158/dehc-qy92.

Sanger, David. E. and Schmitt, Eric. (2015) 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', *The New York Times*. [Online] 25 October 2015. 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 March 2024).

Scott, Mark. (2022) 'Will Russia attack undersea internet cables next?', *Politico*. [Online] 29 September 2022. https://www.politico.eu/article/everything-you-need-to-know-about-the-threat-to-undersea-internet-cables/ (Accessed: 28 February 2024).

Siebold, Sabine. (2023) 'NATO says Moscow may sabotage undersea cables as part of war on Ukraine', *Reuters*. [Online] 3 May 2023. https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/ (Accessed: 28 February 2024).

Soldatkin, Vladimir and Antonov, Dmitry. (2024) 'Putin casts naval exercise with China as bid to counter US in the Pacific', *Reuters* [Online] 10 September 2024.c https://www.reuters.com/world/russia-teams-up-with-china-start-big-naval-drills-2024-09-10/ (Accessed: 11 September 2024).

Stensrud, Cecilie Juul and Østhagen, Andreas. (2024) 'Hybrid Warfare at Sea? Russia, Svalbard and the Arctic', *Scandinavian Journal of Military Studies*, Vol. 7(1), pp. 111–130. https://doi.org/10.31374/sjms.233.

Stent, Angela. (2020) '*Russia and China: Axis of Revisionists? Brookings Series on Global China*. [Online] February 2020. https://www.brookings.edu/articles/russia-and-china-axis-of-revisionists/ (Accessed: 10 September 2024).

Ten Houten, Merien. (2023) 'Russian spy ships: Mapping undersea infrastructure for sabotage?', *Innovation Origins*. [Online] 19 April 2023. https://innovationorigins.com/en/russian-spy-ships-mapping-undersea-infrastructure-for-sabotage/ (Accessed: 28 February 2024).

United States Navy. (2022) 'NATO's Operation Sea Guardian returns to Western Mediterranean', *NATO Allied Maritime Command Public Affairs*. [Online] 14 March 2022. https://www.navy.mil/Press-Office/News-Stories/Article/2965604/natos-operation-sea-guardian-returns-to-western-mediterranean/ (Accessed: 26 June 2024).

Vilnius Summit Communiqué. (2023) Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023. [Online] July 2023. https://www.nato.int/cps/en/natohq/official_texts_217320.htm (Accessed: 19 March 2024).

Wall, Colin and Morcos, Pierre. (2021) 'Invisible and Vital: Undersea Cables and Transatlantic Security', *Center for Strategic and International Studies CSIS* [Online] 11 June 2021. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security (Accessed: 28 February 2024).