IDR
Romanian Diplomatic Institute

Ministerul Afacerilor Externe

POLICY BRIEF no. 76/2025

Crossing the line: Severing undersea internet cables in geopolitical hotspots

Claudiu Codreanu

Crossing the line: Severing undersea internet cables in geopolitical hotspots[1]

Claudiu Codreanu[2]

Researcher

Romanian Diplomatic Institute

ABSTRACT: Recent events in the Baltic Sea and in the Taiwan Strait highlight vulnerabilities in protecting critical infrastructure from intentional and unintentional damage. Undersea internet cables are the hidden nervous system of our digitalised world. Severing one or two cables will not shut down all internet connections in a large region or country, but damaging specific cables can cut down traffic speed or even cause limited internet blackouts. However, showing readiness to cut undersea cables represents a threat to telecommunications worldwide. Alleged actions undertaken by both Russia and China over the last two years show that direct physical sabotage should not be overlooked when it comes to protecting internet infrastructure and cybersecurity. This study discusses the recent incidents regarding undersea internet cables in the Baltic Sea and Taiwan Strait and the role of Russia and China as potential actors trying to sabotage these elements of critical infrastructure. Moreover, the study explores the response taken into consideration by the affected states and by organisations such as NATO and EU. Ultimately, it will propose several recommendations.

KEYWORDS: undersea cables, internet infrastructure, Baltic Sea, Taiwan, Russia, China.

[1] This publication draws exclusively on open-source materials. The opinions expressed herein are solely those of the author and do not necessarily reflect those of the institution.

[2] claudiu.codreanu@idr.ro

INTRODUCTION

There has been an increase in incidents causing damages to undersea cables and pipelines after Russa's full-blown invasion of Ukraine in 2022 (Webster 2025). Russian commercial and military vessels have been sailing close or through Ireland's Exclusive Economic Zone (EEZ) since 2022, and in November 2024 a Russian research vessel has been escorted by Ireland's navy after found patrolling in the area of multiple subsea cables and pipelines between Ireland and the UK (Besch & Brown 2024, 7).

Date	**Location**	**Infrastructure damaged**	**Suspected actor**	**Ship involved**	**Official explanation (Accused actor)**	**Official explanation (Targeted state)**
Feb 2-8, 2023	Taiwan	Two undersea cables	China	Not specified	No official statement	Suspected deliberate damage
Oct 8-10, 2023	Baltic Sea	Balticonnector pipeline, EE-S1 telecom cable	China	Newnew Polar Bear	Accidental damage	Under investigation
Nov 17-18, 2024	Baltic Sea	BCS East-West Interlink & C-Lion1 telecom cables	China	Yi Peng 3	Denial	Under investigation
Dec 25, 2024	Baltic Sea	Estlink 2 power cable & 4 telecom lines	Russia	Eagle S	Denial	Under investigation
Jan 3, 2025	Taiwan	Undersea telecom cable	China	Shunxin 39 (suspected)	Denies involvement	Suspected deliberate damage
Jan 26, 2025	Baltic Sea	C-Lion1 telecom cable	Russia	Vezhen (suspected)	No official statement / denial	Under investigation
Feb 25, 2025	Taiwan	Undersea telecom cable	China	Hongtai	No official statement / denial	Suspected deliberate damage

Table 1. Recent events of undersea infrastructure damaged in the Baltic Sea and Taiwan. Sources: Davidson 2025a; Cater 2025; Chang & McCarthy 2025; Miller, Dixon & Stanley-Becker 2025; Martin 2025c; Hale 2025

Even though the area around Ireland's EEZ hosts several undersea cables linking Europe to the United States, **Russian interest apparently moved to the Baltic Sea, where**

NATO countries neighbouring the sea accused Russia of using commercial vessels to severe multiple cables over the last two years. As expected, Russia denied all accusations. Moreover, the situation around Taiwan is even more complicated, considering China's military escalations in the area (Chang & McCarthy 2025).

The area around Taiwan and the Baltic Sea region have been international hotspots for both geopolitical tensions and incidents regarding undersea infrastructure. As multiple subsea internet and power cables were damaged, as well as a pipeline in the Baltic area, there have been discussions whether these incidents were mere accidents caused by various factors or coordinated acts of sabotage part of hybrid campaigns (Besch & Brown 2024; Davidson 2025a; Cater 2025; Martin 2025a; Astier & Kirby 2024; Khorrami 2025). Nevertheless, these developments are concerning but not heralds of doomsday scenarios.

BACKGROUND

The first copper cable was laid between the United States and the United Kingdom in 1858, allowing the two countries to send telegrams to each other (Sanger 2022). Almost 170 years later, there are over 1.4 million kilometres of undersea internet cables all over the world (Ganz et al. 2024, 2). Notably, targeting submarine cables with sabotage operations is not something new. Back in 1898, the US navy cut a telegraphic cable near Cuba's coast during the Spanish-American war, with the goal of disrupting their communications (Milmo 2024). Sixty years later, in 1959, Washington accused Russia of intentionally damaging an undersea cable with fishing nets (Freund 2025).

Around **99% of the global internet traffic** passes through undersea cables (Ganz et al. 2024, 2; Sanger 2018; European Commission 2025). Besides telecommunications, other undersea cables transport electrical energy and high-voltage direct current between different countries, islands, or connecting to offshore wind turbines (Freund 2025). Cutting some of the main cables would cause country-wide or regional outages and slowdowns, but cutting all of them would destroy global internet (Ganz et al. 2024, 2). **Satellite connections** are not yet a viable alternative to submarine cables, as they are slower, vulnerable to interference, more expensive, and can transfer less amounts of data (Freund 2025).

Responses to such incidents are as vague and unambitious as international regulations go. The United Nations Convention on the Law of the Sea includes several articles governing undersea cables, mostly referring to what actors can and cannot do in international waters, territorial seas, exclusive economic zones and so on (Ganz et al. 2024, 5). However, undersea internet cables are not subject to sufficient protections by existing legal regimes, whilst also setting no concrete accountability for malicious actors (Besch & Brown 2024, 6).

In the meantime, large technology companies are intensifying their efforts for developing **large scale submarine internet cables**, as the majority of cables are owned by private companies (Ganz et al. 2024, 5). Concurrently, companies can influence states' policies regarding internet infrastructure through funding large projects or controlling existing infrastructure, and governments can affect companies as well through regulation, political pressure, and can also capitalize on them to promote their influence abroad (Ganz et al. 2024, 6).

Undersea cables have another vulnerability on par with physical damages – **espionage**. The 2013 Edward Snowden leaks revealed that American and British intelligence agencies infiltrated termination points (the place where cables get on land) to mine and collect data from them, after securing deals with telecom companies operating them (Sanger 2022). Cybersecurity and espionage-related concerns have been raised by European and US officials regarding the undersea cables built and operated by the Chinese-based **Huawei Marine Networks (HMN)** (Besch & Brown 2024). One example is the 2022-built Pakistan and East Africa Connecting Europe (PEACE) cable, going from Europe to Asia, through North Africa and the Middle East. At the beginning of 2024, the European Parliament passed a resolution expressing its concern regarding HMN Tech links to China's People Liberation Army, highlighting potential cybersecurity vulnerabilities (Besch & Brown 2024, 8).

RECENT EVENTS

Baltic Sea

In October 2023, the **Balticonnector** gas pipeline between Finland and Estonia and the EE-S1 telecom cable between Estonia and Sweden were damaged in an apparent accident (Besch & Brown 2024, 8). The incident was caused by a Chinese-owned vessel, Newnew Polar Bear, registered in Hong Kong (Khorrami 2025). In August 2024, **the Chinese government**

admitted that the incident was caused by the vessel, stressing that it was an accident caused by weather conditions (Besch & Brown 2024, 8).

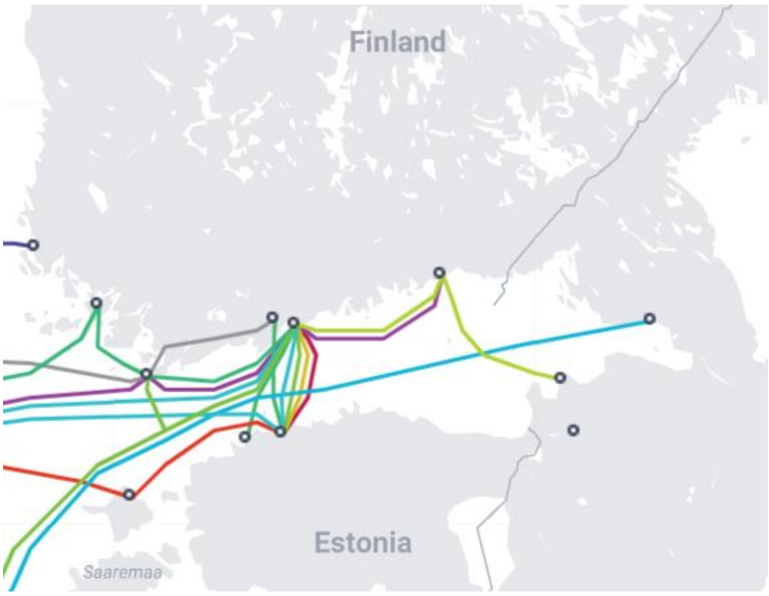

Figure 1. Baltic Sea area submarine cables. Source: Telegeography 2025

In November 17-18, 2024, two submarine telecom cables, the **BCS East-West Interlink**, connecting Lithuania to Gotland, Sweden, and the **C-Lion1**, linking Germany to Finland, have been damaged. Swedish and Dannish authorities identified a vessel suspected of severing the cables, the Chinese-registered Yi Peng 3 cargo ship, which passed the two cables on the same dates (Bryant & Sauer 2024). Evidence from sonar images showed that the vessel dragged its anchor along the seabed for 160 kilometres (Hale 2025). The Yi Peng 3 vessel has been suspected by Germany, Sweden, and Finland, raising the probability of Russian usage of private Chinese assets for its hybrid activities (Khorrami 2025). In this context, German Defence Minister Boris Pistorius stated that there are suspicions of sabotage and hybrid actions (Astier & Kirby 2024). China started its own investigation of the incident, allowing also to board the vessel as "observants" representatives of Denmark, Germany, Finland, and Sweden (Hale 2025). An investigation underdone by the Swedish police is still ongoing (Webster 2025). Nevertheless, intelligence officials cited by media outlets and members of the European Parliament suspected Russian involvement (Besch & Brown 2024, 7-8).

On December 25, 2024, **four undersea internet cables** and the **Estlink 2** power cable between Finland and Estonia were damaged by a Russian-linked oil tanker, the Eagle S, which dragged its anchor along the seabed for 100 kilometres (Borger 2025). The Russian tanker ship, carrying oil from Russia, was seized by Finnish authorities and only allowed to depart in February 2025, whilst its crew members have been placed under a travel ban and the criminal investigation is still ongoing (Khorrami 2025; DW 2025; Hale 2025).

On January 26, 2025, **an undersea internet cable** in the Baltic Sea was damaged in the area between Latvia and Sweden (Cater 2025). The owner of the cable, Latvia's State Radio and Television Center, announced then that delays were limited as traffic has been rerouted (DW 2025). Latvian Prime Minister Evika Siliņa stated that the incident was likely caused by "external influence," as the authorities started investigating three suspected vessels, including by sending a patrol (Cater 2025). Latvia worked closely with Sweden and NATO (Cater 2025). In February 2025, Swedish and Finnish authorities announced they are investigating another incident regarding a damaged Baltic undersea cable, the **C-Lion1**, but it become apparent that the cable had been damaged during the same incident in January (Reuters 2025a; Reuters 2025b).

Taiwan Strait

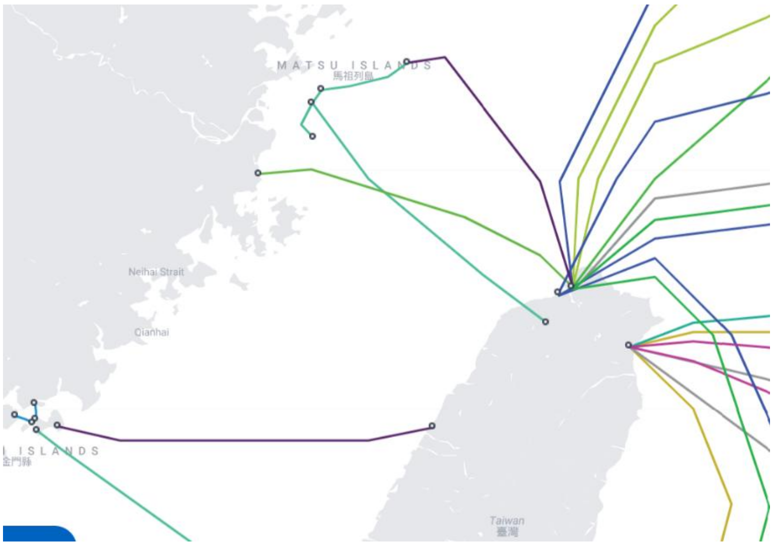

Figure 2. Taiwan Strait area submarine cables. Source: Telegeography 2025

In February 2023, two Chinese vessels were suspected by Taiwanese authorities of severing two undersea cables near the **Matsu islands**, cutting the internet for its residents

(Davidson 2025a). This has been the most serious incident to date, as it caused an **internet blackout in the islands and the need of a costly repair**.

At the beginning of January 2025, an **undersea cable** going from Taiwan to the US was damaged north-east of Taiwan. Services were mostly unaffected, according to Taiwan's Chungwa Telecom, as data was rerouted to other cables (Davidson 2025a). The cable was damaged by a Chinese-linked and Cameroon-registered cargo ship, Shunxin 39, which was detained by Taiwan's authorities after being suspected of dragging its anchor on the seabed in the area of the cable (Davidson 2025a; Chang & McCarthy 2025). The incident is still under investigation and considered as a potential act of sabotage (Davidson 2025a).

On February 25, 2025, another **undersea cable** was damaged in the Taiwan Strait between Taiwan's main island and Penghu (Davidson 2025b). Taiwanese authorities detained a Togolese-flagged and Chinese-crewed cargo ship and started an official investigation without ruling out the possibility of an intentional act of sabotage (Davidson 2025b).

Response and implications

Russia's Eagle S tanker, part of the so-called **shadow fleet**, has been the subject of a criminal investigation opened by Finland in relation to the cable severed during Christmas in 2024 (Cater 2025). Russia's shadow fleet refers to the network of aging tanker ships with obscure ownership helping Russia evade international sanctions by selling its oil on global markets (Miller, Dixon & Stanley-Becker 2025; Jack 2025). Estonia, Finland, Latvia, and Lithuania have been considering legal mechanisms through which they could detain vessels part of Russia's shadow fleet (Jack 2025).

In another case, Swedish authorities released the Bulgarian-owned Vezhen cargo ship in early February 2025, after it was seized in connection to the January 26 incident, stating that the ship is suspected of having damaged the cable but the case is not an act of sabotage and rather an accident caused by weather conditions (Martin 2025c). However, Swedish Prime Minister Ulf Kristersson argued during the 2025 Munich Security Conference that **the series of undersea cable cuts cannot be ruled out as simply coincidental, as it may be part of hybrid tactics** (Martin 2025b).

In January 2025, **NATO** Allies bordering the Baltic Sea issued a statement condemning the acts of sabotage against undersea infrastructure, as well as stating that they reserve their rights to take action against ships involved in such incidents (Martin 2025a). NATO's role in protecting critical infrastructure and its presence in the Baltic Sea became evident in late 2024. Worth mentioning here are NATO's naval patrols in the Baltic Sea, starting in late December 2024, and the Alliance's Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications (HEIST), the latter aiming to assure the rerouting of internet traffic to space in the event of critical damage done to undersea cables (Khorrami 2025; NATO 2024; Besch & Brown 2024). Mid-January 2025, NATO launched a mission to protect critical infrastructure in the Baltic Sea, deploying frigates, naval drones, as well as aircraft (DW 2025). Nevertheless, threats and risks regarding undersea infrastructure have been long known by the Alliance. In early 2023, NATO established the Critical Undersea Infrastructure Coordination Cell, aiming at enhancing cooperation between states and private actors and assess vulnerabilities in this sector (Besch & Brown 2024, 14).

As for Taiwan, the situation is much more complicated than that in Europe. **In the case that an actor managed to cut off all the undersea internet cables connecting Taiwan internationally, the country will have to rely only on satellites, causing a major disruption of its society, economy, trade and so on** (Chang & McCarthy 2025). The incidents around Taiwan can be considered part of hybrid interferences, low-level operations that undermine and harass the state and its citizens, or as setting the ground and testing for large scale attacks in the future, given the tensions in the area (Chang & McCarthy 2025).

Up to this date, **the response is still rather vague**, including the attributions of the countries involved, as investigations are still ongoing and it is not clear whether some or all these incidents are deliberate acts of sabotage or mostly accidental events. EU's Action Plan on Cable Security, published in February 2025, suggests that **the pattern observed lately indicates that undersea infrastructure has become the target of "deliberate hostile acts" that can be considered elements of broader hybrid campaigns** (European Commission 2025, 1). The plan identifies these actions as acts of sabotage representing "significant risks to the security of the EU" (European Commission 2025, 1). However, *The Washington Post* reported in January 2025 that the consensus building among US and European intelligence agencies is that the series of incidents involving undersea cables has been caused by **accidents** and not deliberate sabotage acts (Miller, Dixon & Stanley-Becker 2025). Thus, there have been conflicting reports and statements from European officials, which suggests that both the investigations and intelligence assessments are not conclusive enough.

CONCLUSIONS AND RECOMMENDATIONS

A complete breakdown of internet connections in Europe caused by cutting undersea cables is extremely unlikely, as there are enough alternative routes that can provide continued coverage (Besch & Brown 2024, 5). However, island countries such as Ireland, Cyprus, or Malta, as well as various islands part of other states, are more vulnerable due to their dependency on undersea cables (Besch & Brown 2024, 5). Thus, malicious actors could sabotage cables to undermine governments, cause economic loss to the private sector, and foster public distrust in institutions and security by producing local blackouts and slowdowns, or testing the ground for a larger attack (Besch & Brown 2024, 5).

The developments around undersea internet cables are dangerous, but they will not lead to doomsday scenarios of global internet destruction. Similar to cyberattacks, the risk of a dooming event such as a major long-term internet outage is low, but it does not mean that governments should not prepare for such a scenario. They can still cause serious disruption alongside other hybrid actions, undermining governments and societies, or disturbing economic activities. Severing one or two undersea cables will not bring down the internet in a whole country, but it can disrupt telecom companies and create unnecessary million-dollar expenses for private and public actors.

Even though some of the incidents in the Taiwan area and Baltic Sea seem to have been costly accidents, not all of them have been completely ruled out for sabotage. **It is unlikely that the whole series of incidents represents only a long chain of accidents**. Public attribution in this case is similar to attributing malicious cyber operations, as both acts can be put under the label of sabotage activities. Even though there is no concrete proof (yet) that Russia and/or China decided to deliberately use commercial vessels to sabotage critical undersea infrastructure, a similar pattern to acts of hybrid interferences becomes visible. At the same time, some of these incidents can represent simple accidents, as there have been several cases when undersea cables have been damaged from naval accidents and even natural causes.

Overall, these kinds of activities enter the 'grey zone' or hybrid influence area of malicious operations, closer to sabotage activities rather than warfare – undermining targeted states, pestering authorities, imposing unnecessary costs without concrete consequences (e.g., millions of euros required for repairing some cables affected), and so

on. As in the case of offensive cyber operations, the main goal seems to be undermining the targeted state's sovereignty, authority, and security, and not causing catastrophic losses or preparing for a full-blown war. Nevertheless, these operations serve as posturing – signalling disposition to damage critical infrastructure in peacetime or employing large-scale attacks during wartime.

Thus, there is need for both **physically protecting the cables and protecting them digitally from cyberattacks, as well as safeguard them from espionage activities**. Moreover, states should punish actors that tamper with them, at least similarly to how states usually respond to cyber operations: **public attribution, international sanctions, and/or criminal cases**. Furthermore, there should be thorough checks and investigations on **private-only developments**, especially in the case of HMN Tech and similar companies. Europe should also keep in check and maintain a balance in dependencies on US-based undersea cable projects and US-based tech companies, judging by the latest developments regarding Starlink and similar companies (The Economist 2025).

EU's recommendations on these issues are crucial in this sense. Both the EU's Digital Operational Resilience Act (DORA) and the Network and Information System 2 Directive (NIS2) put forward courses of action for securing submarine cables infrastructure (Khorrami 2025). Moreover, **EU's Action Plan on Cable Security** proposes the usage of the Union's Hybrid Toolbox, which included responses such as public statements of joint attributions or harnessing EU's sanctions regime (European Commission 2025, 15). Other measures proposed by the Action Plan include enhancing EU's capabilities of responding to Russia's shadow fleet, bolstering its capabilities of holding accountable malicious actors, strengthening cooperation with NATO on this issue, and boosting strategic communication on cable security and hybrid threats (European Commission 2025, 17).

As for **Romania**, the only undersea telecom cable in Romania's EEZ is the KAFOS cable. Its landing points are Mangalia (Romania), Varna (Bulgaria), Igneada (Türkiye), and Istanbul (Türkiye). The node in Istanbul connects the cable to the MedNautilus Submarine System, which connects several countries: Cyprus, Greece, Israel, Italy, and Türkiye. The only other undersea cables in the Black Sea are the Caucasus Cable System (Bulgaria-Georgia), the Georgia-Russia telecom cable, and the two cables in the Kerch Strait, connecting Russia's Krasnodar Krai to the Russian illegally-occupied Crimea.

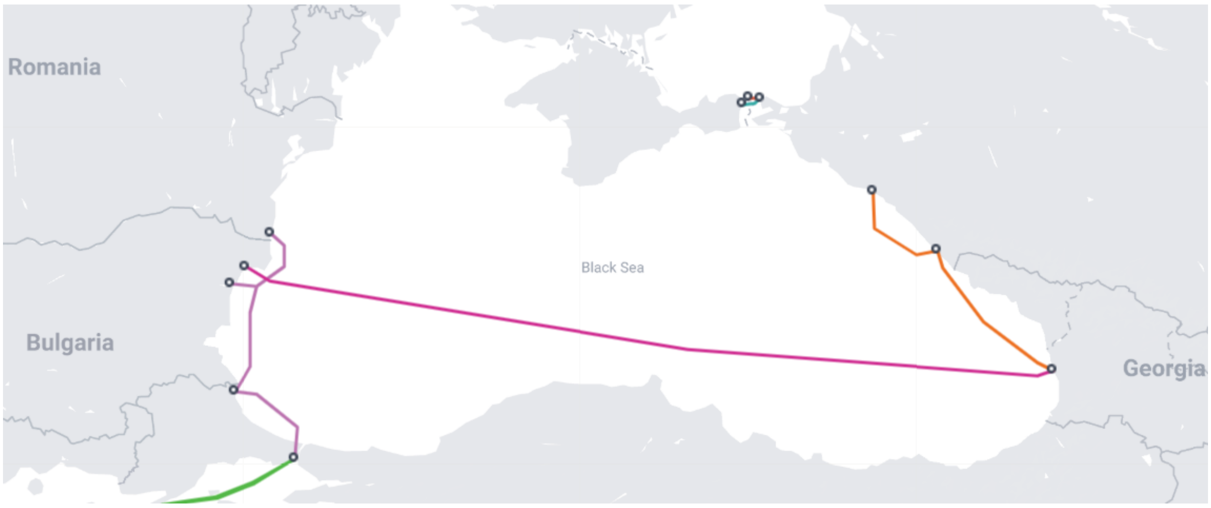

Figure 3. Black Sea area submarine cables. Source: Telegeography 2025

Therefore, Bucharest's main role in this case is to offer support to countries near the Baltic Sea, as the Black Sea area has not been a hotspot for these kinds of incidents, despite Russia's war of aggression against Ukraine. Romania should implement the EU's Action Plan recommendations to the cable in its EEZ and regarding the landing station in Mangalia, as well as enhance cooperation with its partners in the Black Sea area and support its allies in the Baltic Area.

BIBLIOGRAPHY

Astier, H., & Kirby, P. (2024, November 19). Germany suspects sabotage over severed undersea cables in Baltic. *BBC*. https://www.bbc.com/news/articles/c9dl4vxw501o

Besch, S., & Brown, E. (2024, December 16). Securing Europe's Subsea Data Cables. *Carnegie*. https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en.

Borger, J. (2025, January 19). Nato flotilla assembles off Estonia to protect undersea cables in Baltic Sea. *The Guardian*. https://www.theguardian.com/world/2025/jan/19/nato-flotilla-assembles-off-estonia-protect-undersea-cables-baltic-sea

Bryant, M., & Sauer, P. (2024, November 20). Swedish police focus on Chinese ship after suspected undersea cable sabotage. *The Guardian*.

https://www.theguardian.com/world/2024/nov/20/sweden-denmark-undersea-cable-sabotage-navy-investigation

Burgess, M. (2022, November 2). The Most Vulnerable Place on the Internet. *Wired*. https://www.wired.com/story/submarine-internet-cables-egypt/

Cater, L. (2025, January 26). Baltic undersea cable likely damaged by 'external influence,' Latvian broadcaster says. *Politico*. https://www.politico.eu/article/baltic-undersea-cable-damaged-external-influence-latvia/

Chang, W., & McCarthy, S. (2025, January 10). A cut undersea internet cable is making Taiwan worried about 'gray zone' tactics from Beijing. *CNN*. https://edition.cnn.com/2025/01/09/china/undersea-cable-taiwan-intl-hnk/index.html

Davidson, H. (2025a, January 7). Taiwan investigating Chinese vessel over damage to undersea cable. *The Guardian*. https://www.theguardian.com/world/2025/jan/07/taiwan-investigating-chinese-vessel-over-damage-to-undersea-cable

Davidson, H. (2025b, February 25). Taiwan detains Chinese-crewed cargo ship after undersea cable damaged. *The Guardian*. https://www.theguardian.com/world/2025/feb/25/taiwan-detains-chinese-crewed-cargo-ship-after-undersea-cable-damaged

DW (2025, January 27). Latvia: Undersea cable likely damaged by external influence. *DW*. https://www.dw.com/en/latvia-sweden-cable-damage-nato/a-71416470

European Commission (2025, February 21). EU Action Plan on Cable Security. *European Commission JOIN(2025) 9 final*. https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables

Freund, A. (2025, March 2). How sabotage on undersea cables affects our digital world. DW. https://www.dw.com/en/how-sabotage-attacks-on-undersea-cables-affect-our-digital-stability/a-71494600

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines*, *34*(3), 31. https://doi.org/10.1007/s11023-024-09683-z

Hale, E. (2025, March 10). As undersea cables break off Europe and Taiwan, proving sabotage is tough. *Al Jazeera*. https://www.aljazeera.com/news/2025/3/10/as-undersea-cables-break-down-proving-sabotage-a-difficult-task

Jack, V. (2025, February 11). Russia lashes out at EU plans to seize its 'shadow fleet' in the Baltic Sea. *Politico*. https://www.politico.eu/article/russia-lashes-out-against-eu-plans-to-seize-its-shadow-fleet-in-the-baltic-sea/

Khorrami, N. (2025, January 9). Subsea sabotage should spark review of critical infrastructure security. *Binding Hook.* https://bindinghook.com/articles-binding-edge/subsea-sabotage-should-spark-review-of-critical-infrastructure-security/

Martin, A. (2025a, January 14). Russia warned its 'shadow fleet' could face action from NATO allies. *The Record*. https://therecord.media/baltic-nato-allies-warning-russia-shadow-fleet

Martin, A. (2025b, February 15). Sweden's PM on suspected cable sabotage: 'We don't believe random things suddenly happen quite often'. *The Record.* https://therecord.media/sweden-pm-on-suspected-russian-cable-breaks-not-an-accident

Martin, A. (2025c, February 3). Sweden releases suspected ship, says cable break 'clearly' not sabotage. *The Record*. https://therecord.media/sweden-releases-ship-suspected-cable-sabotage

Miller, G., Dixon, R., & Becker-Stanley, I. (2025, January 19). Accidents, not Russian sabotage, behind undersea cable damage, officials say. *The Washington Post*. https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/

Milmo, D. (2024, November 22). Wire cutters: How the world's vital undersea data cables are being targeted. *The Guardian*. https://www.theguardian.com/world/2024/nov/22/wire-cutters-how-the-worlds-vital-undersea-data-cables-are-being-targeted

NATO (2024, August 28). *NATO-funded project to reroute internet to space in case of disruption to critical infrastructure*. *NATO*. https://www.nato.int/cps/en/natohq/news_228257.htm

Reuters (2025a, February 21). Finland, Sweden investigate suspected sabotage of Baltic Sea telecoms cable. *Reuters*. https://www.reuters.com/world/europe/sweden-investigates-possible-breach-undersea-cable-baltic-sea-prime-minister-2025-02-21/

Reuters (2025b, February 24). Damage to Baltic Sea telecoms cable may have occurred in January, operator says. *Reuters*. https://www.reuters.com/world/europe/damage-baltic-sea-telecoms-cable-may-have-occurred-january-operator-says-2025-02-24/

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age* (First edition). Crown Publishing Group.

Telegeography (2025). *Submarine Cable Map*. Retrieved 2 April 2025, from https://www.submarinecablemap.com/

The Economist (2025, March 13). Could Europe replace Starlink if America pulls the plug? *The Economist*. https://www.economist.com/international/2025/03/13/could-europe-replace-starlink-if-america-pulls-the-plug

Wall, C., & Morcos, P. (2021, June 11). Invisible and Vital: Undersea Cables and Transatlantic Security. CSIS. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Webster, E. (2025, February 21). Sweden investigates suspected sabotage of undersea telecoms cable. *BBC*. https://www.bbc.com/news/articles/cy5nydr9rqvo

IDR

Institutul Diplomatic Român

Our mission. The Romanian Diplomatic Institute (RDI) has the mission to make a substantial contribution to increasing the quality of Romanian diplomacy through training, further education, research, the development of critical and strategic thinking and international networking. A good foreign policy serves as a beneficial domestic policy.

Guiding principles: human resource development, professionalism, respect and dialogue, and responsibility for the community.

Based on the founding legal attributions of the RDI, the further development of the Institute is carried out, according to the needs identified in the MFA, along the following four directions:

- Training and further education of diplomats and other trainees;
- Deepening the research and expertise dimension on regional and functional issues;
- Operating the RDI as a think-tank of the MFA;
- Integration of the RDI into an international network of similar relevant institutes.

Author: Claudiu Codreanu (PhD) is a researcher at the Romanian Diplomatic Institute – Department of Expert Analysis.

RDI Policy Brief Series

ISSN 2066-5989

ISSN-L 2066-5989

Cover photo:

https://commons.wikimedia.org/wiki/File:Telstra_submarine_cable_caution_sign,_Milsons_Point.jpg

The Romanian Diplomatic Institute

https://www.idr.ro/en/ | secretariat@idr.ro

Primăverii 17, Sector 1, Bucharest, 011972