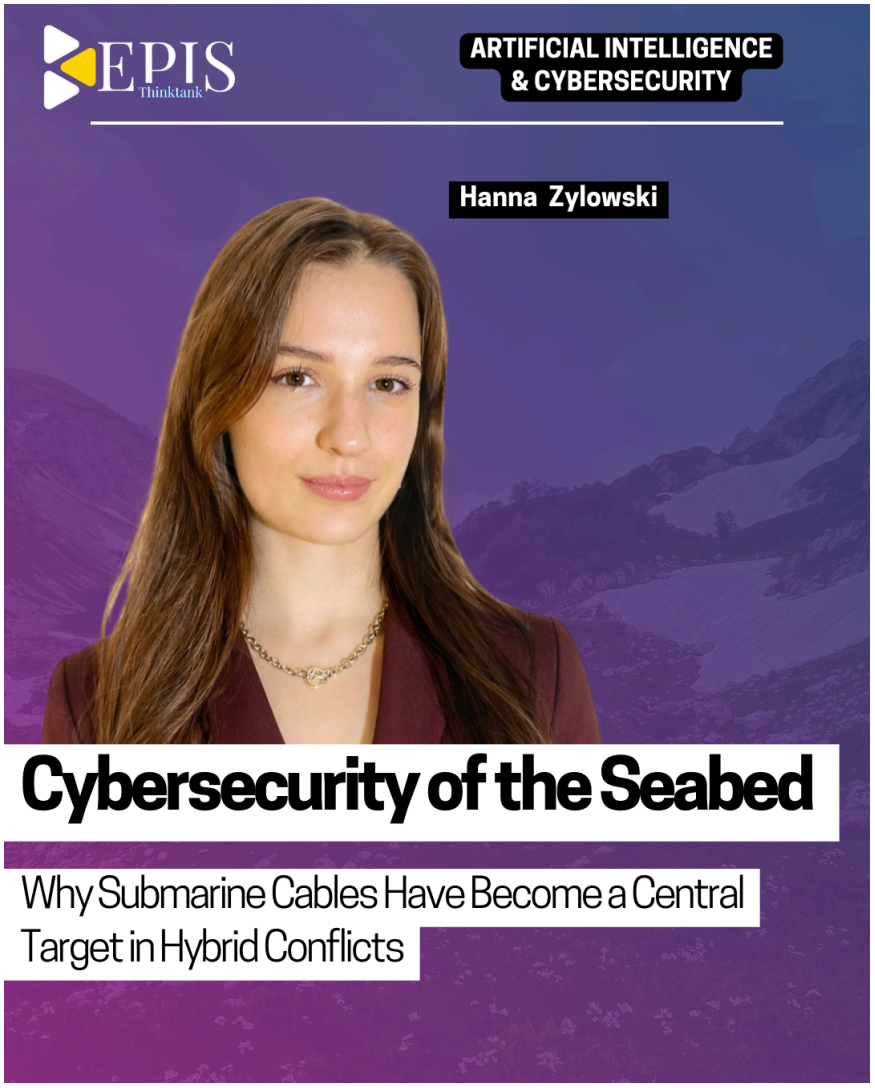

About the Author:

Hanna Zylowski

Hanna Zylowski has a background in International Relations with a particular interest in security studies, hybrid threats, and international cooperation. She is motivated by the belief that Europe stands at a pivotal moment and aims to contribute to innovative solutions for the challenges shaping its future.

About the publication:

3 Main Points:

How vulnerable are Europe's submarine cables to hybrid threats, and what does this

mean for maritime cybersecurity? The analysis shows that physical exposure, digital weaknesses and governance gaps make cables key targets for state-linked actors. Protecting them requires stronger monitoring, shared EU-NATO coordination and higher cybersecurity standards.

Cybersecurity of the Seabed:

Why Submarine Cables Have Become a Central Target in Hybrid Conflicts

Increasing geopolitical tension and rapid digitalisation are turning maritime space into a tangled security landscape. Physical infrastructure, digital systems and information flows are increasingly intertwined, creating new points of vulnerability that extend far beyond the visible surface. The stability of Europe's underwater networks, however, has emerged as a key issue in this regard, as disruptions carry immediate political, economic and strategic implications.

Submarine cables are some of the least visible but most strategically vital pieces of infrastructure in the world today. Some 97 to 99 per cent of all international internet and data traffic passes through these fibre optic cables very deep in the ocean floor (EU Digital Strategy 2024; ITU 2024). These cables are vital but very difficult to monitor since the cables are poorly protected and mostly located in international waters where no clear jurisdiction exists (EUISS 2023). With the advent of digitalisation, the need for stable data connections increases, meaning that even a single upheaval can have crippling consequences on the economy, government and international security. State-linked actors have also shown interest in submarine cables through sabotage, reconnaissance or digital access to control and monitoring systems (ICPC 2022; NATO 2023). The susceptibility of deep-sea cables is no longer only a technical issue but rather is becoming a security and political threat. Hence, an examination of their vulnerabilities and protective mechanisms is crucial for future maritime security (EUISS 2024; Cattler 2024).

How Subsea Cables Work and Why They Matter

Each cable has multiple layers of protection around a thin fibre core that conducts data through a series of light pulses. The undersea cable and terrestrial networks connect at both ends via landing stations. Their operation relies on optical amplifiers, control software and constant digital analysis with digital monitoring (ITU 2024; JRC 2025). There are three primary reasons why subsea cables are at risk. First, they can be physically exposed: many cables run unprotected for thousands of kilometres along the seafloor, making them receptive to damage by sabotage, anchors or fishing (EUISS 2023). Second, landing stations, control software and monitoring platforms can be attacked from cyberspace, given they are frequently privately owned and often have varying security standards (ITU 2024). Third, there are ongoing gaps in governance. International waters have very few means of legitimate enforcement, with no state holding out clear authority to safeguard or supervise vast stretches of cable (EU Digital Strategy 2024). This conjunction of hazards makes deep-sea cables in particular susceptible to hybrid attacks.

Technical, Cyber and Governance Vulnerabilities

Cybersecurity threats are spreading to various sectors of the sea. Ports and logistics systems suffer attacks and can disrupt whole operations (ENISA 2020). Digitalisation also leaves navigation systems and digital controls vulnerable; for example, altered software or networked boards have a direct impact on ship handling (Kechagias 2022). Offshore energy installations are also vulnerable, as their industrial control systems have become increasingly connected and thus exposed to digital interference (Mohammed 2022).

Additionally, the growing importance of undersea networks cannot be dismissed. Their landing stations and monitoring systems are considered particularly sensitive because they are indispensable for global data traffic, and they can be targeted and attacked as well (European Parliament 2022; ENISA 2023).

Collectively, these findings show that a wide range of maritime systems are increasingly facing serious cybersecurity challenges.

Recent Incidents and Windows of Cyber Exploitation

Cable failures are not isolated risks but common occurrences. Such is the case in the Shetland and Faroe Islands, where fibre optic cables were destroyed in October 2022 in the North Atlantic, leaving much of the population at least temporarily without stable internet and, in some cases, without access to landlines. They called it a “major incident”, and restoration took days (BBC 2022). Multiple fibre cables in southern France were also cut. Investigators warned of deliberate destruction and opened an investigation into sabotage (Reuters 2022; RFI 2022; DataCenterDynamics 2022).

From a cybersecurity perspective, such incidents create a window of vulnerability. When the network already is under pressure, it tends to be easier to disguise DDoS attacks: routing manipulation like one involving BGP hijacking is easily overlooked, and overwhelmed monitoring and incident response services react more slowly. Research into the threat situation at sea shows that attackers take advantage of these stressful moments to infiltrate malware or gain access to land stations and control systems (Cloudflare 2024).

Hybrid Threats: State Reconnaissance and Strategic Pressure

This leads directly to the discussion of hybrid threats, in which Russia is frequently identified as a central actor (EUISS 2023; Hybrid CoE 2025; Foreign Affairs 2023). The Russian navy and related “research” ships systematically survey underwater networks in Europe, including cables, power lines and pipelines. Recent reports point to Russian vessels sailing subsea cable routes and conducting reconnaissance in European waters (DataCenterDynamics 2025; WTOP 2025). Investigations also reveal Russian naval activity around the Nord Stream explosion

locations, a finding indicative of a broader trend of underwater intelligence activities aligned with hybrid operations (Whit 2023).

Several policy analyses indicate Russia is realising that submarine cables are just another strategic tool to apply pressure. These include covert reconnaissance, prepositioning targets and plausible sabotage that can look like an accident (EPRS 2022; EUISS 2023; Hybrid CoE 2025). Russia is conducting reconnaissance of underwater infrastructure through its “research vessels”, e.g., the Yantar, and is developing a growing shadow fleet that blends military operations with civil services (EUISS 2023; EPC 2024; Foreign Affairs 2023). Analysts outline scenarios where Russia specifically damages individual cables in the North Atlantic or the Baltic Sea as well as their vulnerability without crossing a threshold of open attack in order to bring uncertainty and economic pressure and test NATO’s response (Hybrid CoE 2025; NATO Defence College 2023).

This kind of cyber-based prepositioning, the quiet building of access to digital control systems, allows attackers to move rapidly and easily in case of an emergency. Espionage, malware injection, or attempts to exploit vulnerabilities in remote access systems are common targets (EPRS 2022; ENISA 2023) within ground stations and network operations centres. Such activities rarely leave clear imprints and may not be detected until months or years later.

Real-life events underscore how closely physical and digital risks are connected. The 2022 Shetland cable outages and sabotage, including near Marseille, caused regional outages and temporarily reduced digital monitoring of the affected routes (NYT 2022; Shetland News 2025; Shetland Times 2025; Heise 2023). Overloaded networks and broken monitoring systems allow for easier disguise of DDoS attacks or route manipulation. This interaction is increasingly seen as a central part of hybrid threats. Hybrid threats focus less on destruction and more

on strategic uncertainty (Hybrid CoE 2025; Foreign Affairs 2023). A single temporary halt in a transatlantic cable could slow down communication between the European government and the US Army and military institutions (EPRS 2022; EUISS 2023; Atlantic Council 2024). When combined with disinformation, including presenting sabotage as a "technical error", this leads to a lack of information that affects decision-making (Hybrid CoE 2025; Politico 2024; Forbes 2025).

Future threat activity is expected to concentrate in the North Atlantic, the North Sea and the Baltic Sea, which are of high geopolitical tension with extensive cables (Atlantic Council 2024; EUISS 2023; EPC 2024). As Russia brings hybrid pressure on Europe, China is growing and globalising its network of cables, operator structures and technology partners (EPRS 2022; Foreign Affairs 2023; EPC 2024). Both trends provide increased likelihood that attacks by cyber actors using submarine cables would become a new weapon in geopolitical competition (Hybrid CoE 2025; EPRS 2022).

Strengthening Resilience: Priorities for the EU and NATO

To increase resilience, maritime surveillance, cyber security, and international cooperation must become more interconnected (EUISS 2023; Hybrid CoE 2025; Atlantic Council 2024). Monitoring the underwater space constantly is essential, as the current systems often have detection gaps (European Union 2025). This encompasses sensor-based maritime reconnaissance and satellite-ship traffic data integration (Hybrid CoE 2025). Another requirement is mandatory cybersecurity standards for landing stations. The EU's Recommendation (EU) 2024/779 lays out minimum requirements for the operators of critical infrastructure, specifically tighter access controls, regular security audits and consistent patch management (Commission Recommendation 2024). These should be compulsory for cable operators and complemented by joint CERT capacity (Cattler 2024).

Since the security of deep-sea cables crosses borders, the EU and NATO need a unified permanent system that includes maritime situation reports, technical data, and cyber threat analysis (Hybrid CoE 2025; Cattler 2024). Europe also needs to augment redundancy by making more cable routes and alternative landing points. The European Commission cautions that too few redundant connections represent a “structural risk” with “immediate economic consequences” of its own (JRC 2025). Island areas in particular require more cables or more robust satellite networks.

The protection of deep-sea cables is therefore not only a technical matter but a key cybersecurity policy concern for the coming years.

References

Atlantic Council. (2024). How the Baltic Sea nations have tackled suspicious cable cuts. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/

Atlantic Council. (n.d.). Threats to the global maritime order. Atlantic Council. https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/transatlantic-security-initiative/threats-to-the-global-maritime-order/

Borko, D. (2018). Cyber security in maritime transport. Hrcak / University of Zagreb. https://hrcak.srce.hr/file/320814

Carnegie Europe. (2024). Securing Europe's subsea data cables. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en

CBS News. (2024). Russia's alleged hybrid warfare against undersea cables. CBS News. https://www.cbsnews.com/news/russia-alleged-hybrid-warfare-undersea-cables/

CCDCOE. (2025). Policy brief on subsea infrastructure and security. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf

Cloudflare. (2024). What is BGP hijacking. Cloudflare Learning Center. https://www.cloudflare.com/en-gb/learning/security/glossary/bgp-hijacking/

Cloudflare. (2024). What is a DDoS attack. Cloudflare Learning Center. https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

DataCenterDynamics. (2022). Saboteurs cut fiber cables in France in second incident this year. DataCenterDynamics. https://www.datacenterdynamics.com/en/news/saboteurs-cut-fiber-cables-in-france-in-second-incident-this-year/

DataCenterDynamics. (2025). Russian spy ship appears to surveil subsea cables in UK waters. DataCenterDynamics.

https://www.datacenterdynamics.com/en/news/russian-spy-ship-appears-to-surveil-subsea-cables-in-uk-waters-shines-lasers-at-military-jets/

Dgtl Infra. (n.d.). Submarine cables: How fiber links power the internet. Dgtl Infra. https://dgtlinfra.com/submarine-cables-fiber-link-internet/

ENISA. (2020). Guidelines on cyber risk management for ports. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

ENISA. (2023). Undersea cables – what is at stake. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf

European Commission Joint Research Centre. (2025). Subsea cables: How vulnerable are they and can we protect them. JRC Explains. https://joint-research-centre.ec.europa.eu/jrc-explains/subsea-cables-how-vulnerable-are-they-and-can-we-protect-them_en

EUISS. (2023). The changing submarine cables landscape. EU Institute for Security Studies. https://www.iss.europa.eu/publications/briefs/changing-submarine-cables-landscape

European Parliament. (2022). Security threats to submarine cables. European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

EPC. (2024). Europe's security begins at sea: It is time to counter Russia's shadow fleet. European Policy Centre. https://www.epc.eu/publication/europes-security-begins-at-sea-its-time-to-counter-russias-shadow-fleet/

Forbes. (2025). The law does not protect undersea cables. Russia and China know it. Forbes. https://www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it

Foreign Affairs. (2023). Moscow's offshore menace. Foreign Affairs. https://www.foreignaffairs.com/united-states/moscows-offshore-menace

Google. (n.d.). Security and DNS: Protecting Google Public DNS. Google Developers. https://developers.google.com/speed/public-dns/docs/security

Guardian. (2022a). Shetland loses telephone and internet services after subsea cable damaged. The Guardian. https://www.theguardian.com/uk-news/2022/oct/20/shetland-loses-telephone-internet-services-subsea-cable-damaged

Guardian. (2022b). Telephone and internet restored in Shetland after cable damage. The Guardian. https://www.theguardian.com/uk-news/2022/oct/21/telephone-and-internet-restored-in-shetland-after-cable-damage

Heise Online. (2023). Renewed sabotage of fiber optic networks in France. Heise. https://www.heise.de/en/news/Renewed-sabotage-of-fiber-optic-networks-in-France-9816918.html

Hybrid CoE. (2025). Hybrid threats to critical underwater infrastructure. European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf

International Telecommunication Union. (2024). Digital resilience of submarine cables. ITU. https://www.itu.int/digital-resilience/submarine-cables/

Kechagias, D. (2022). Cyber security of maritime autonomous surface ships. Journal article, ScienceDirect. https://pdf.sciencedirectassets.com/…/S1874548222000166/main.pdf

Le Monde. (2025). Russian secrets: How Russia built an Arctic spy network using European equipment. Le Monde. https://www.lemonde.fr/en/les-decodeurs/article/2025/10/23/russian-secrets-how-russia-built-an-arctic-spy-network-using-european-equipment_6746699_8.html

Maritime Cybersecurity. (n.d.). Maritime cyber security information portal. Maritime Cybersecurity. https://www.maritime-cybersecurity.com/

Mohammed, A. (2022). Cyber security challenges of offshore energy control systems. arXiv preprint. https://arxiv.org/pdf/2202.12179

New York Times. (2022). Shetland suffers communications outage after undersea cable damage. The New York Times. https://www.nytimes.com/2022/10/20/world/europe/shetland-scotland-outage.html

NATO Defence College. (n.d.). Russia's strategy for the development of marine activities to 2030. NATO Defence College. https://www.ndc.nato.int/russias-strategy-for-the-development-of-marine-activities-to-2030/

NPR. (2024). Finland points to Russia after severed undersea cable and shadow fleet activity. National Public Radio. https://www.npr.org/2024/12/31/nx-s1-5243302/finland-russia-severed-undersea-cable-shadow-fleet

Politico. (2024). Russia suspected of sabotage of undersea cables in the Baltic Sea. Politico Europe. https://www.politico.eu/article/russia-sabotage-undersea-cables-baltic-sea-europe-war/

Press and Information Office of the United Nations. (2023). Security Council discusses Nord Stream pipeline explosions. United Nations. https://press.un.org/en/2023/sc15231.doc.htm

Reuters. (2022). Internet outages in several French cities as operator cites acts of vandalism. Reuters. https://www.reuters.com/world/europe/internet-outages-several-french-cities-free-cites-acts-vandalism-2022-04-27/

Reuters. (2024). Telecoms cable linking Finland and Germany likely severed, owner says. Reuters. https://www.reuters.com/business/media-telecom/telecoms-cable-linking-finland-germany-likely-severed-owner-says-2024-11-18/

RFI. (2022). France investigates suspected sabotage of fiber optic cables that disrupted internet. Radio France Internationale.

https://www.rfi.fr/en/science-and-technology/20220428-france-investigates-suspected-sabotage-of-fiber-optic-cables-that-disrupted-internet

Shetland News. (2025). Damage to vital communication links causes disruption in Shetland. Shetland News. https://www.shetnews.co.uk/2025/11/27/damage-vital-communication-links-caused/

Shetland Times. (2025). Partnership approach needed to prevent connectivity issues. The Shetland Times. https://www.shetlandtimes.co.uk/news/partnership-approach-needed-to-prevent-connectivity-issues-420033/

The Atlantic Council / Jill Goldenziel. (2025). The law does not protect undersea cables. Forbes. https://www.forbes.com/sites/jillgoldenziel/2025/02/13/law-doesnt-protect-undersea-cables-russia-and-china-know-it

The Guardian. (2022). Shetland loses telephone and internet services after subsea cable damaged. The Guardian. https://www.theguardian.com/uk-news/2022/oct/20/shetland-loses-telephone-internet-services-subsea-cable-damaged

UN Security Council. (2023). Press release on attacks against undersea infrastructure. United Nations. https://press.un.org/en/2023/sc15231.doc.htm

Wired. (2018). The untold story of NotPetya, the most devastating cyber attack in history. Wired Magazine. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

WTOP. (2025). Russian spy ship exposed off UK coast, crew take aggressive action. WTOP. https://wtop.com/j-j-green-national/2025/11/analysis-russian-spy-ship-exposed-off-uk-coast-crew-take-aggressive-action/

YouTube / European institution. (n.d.). Talk on subsea cables and hybrid threats. YouTube. https://www.youtube.com/watch?embeds_referring_euri=https%3A%2F%2Fwe

btools.europa.eu%2F&source_ve_path=Mjg2NjQsMTY0NTAz&v=SL8HGcJxZak&feature=youtu.be