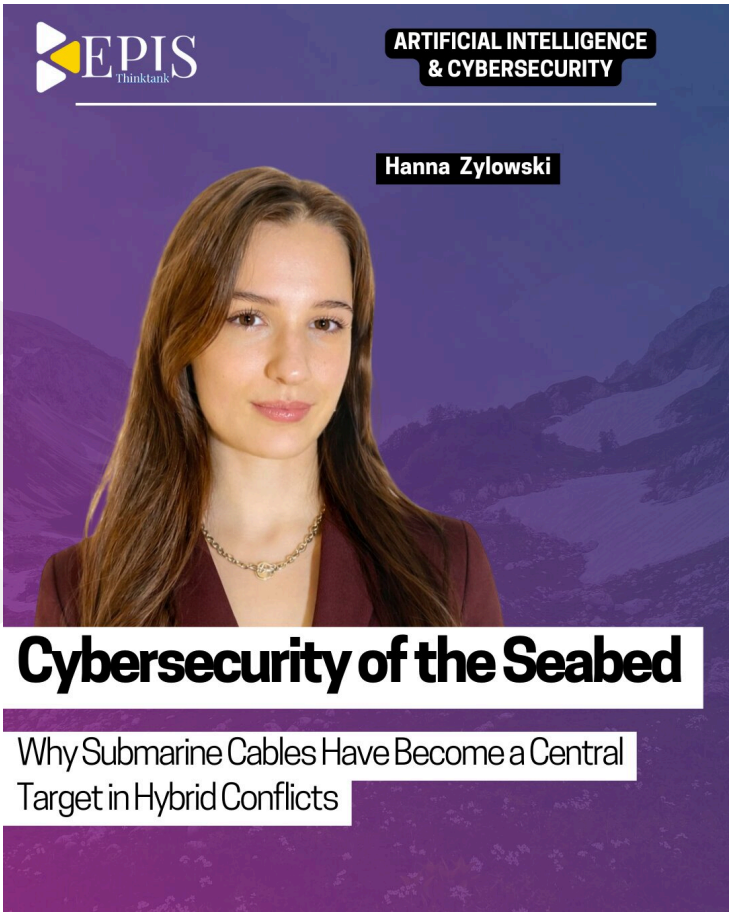
Cybersecurity of the Seabed

30 NOVEMBER 2025

Hanna Zylowski



Cybersecurity of the Seabed:

Rising 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 has emerged as a key issue in this regard, since disruptions carry immediate political, economic and strategic implications.

Submarine cables are among the least visible yet 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 fibre optic cables laid deep on the ocean floor (EU Digital Strategy 2024; ITU 2024). These cables are vital but very difficult to monitor, as they are poorly protected and mostly located in international waters where no clear jurisdiction exists (EUISS 2023). As digitalisation advances, the need for stable data connections grows, meaning that even a single disruption can have crippling consequences for 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 vulnerability of deep-sea cables is therefore no longer purely a technical issue but is increasingly becoming a security and political concern. An examination of their vulnerabilities and protective mechanisms is thus crucial for future maritime security (EUISS 2024; Cattler 2024).

How Subsea Cables Work and Why They Matter

Each cable consists of multiple protective layers around a thin fibre core that transmits data through pulses of light. The undersea cable connects to terrestrial networks at both ends via landing stations, and its operation relies on optical amplifiers, control software and continuous digital monitoring (ITU 2024; JRC 2025). There are three main reasons why subsea cables are at risk. First, they are physically exposed: many run unprotected for thousands of kilometres along the seafloor, making them susceptible to damage from sabotage, anchors or fishing activity (EUISS 2023). Second, landing stations, control software and monitoring platforms are vulnerable to cyberattacks, since they are frequently privately owned and vary widely in security standards (ITU 2024). Third, significant gaps remain in governance: international waters offer very limited means of enforcement, and no state holds clear authority to protect or oversee vast stretches of cable (EU Digital Strategy 2024). Together, these factors make deep-sea cables particularly susceptible to hybrid attacks.

Technical, Cyber and Governance Vulnerabilities

Cybersecurity threats extend across various sectors of the maritime domain. Ports and logistics systems have suffered attacks capable of disrupting entire operations (ENISA 2020). Digitalisation has also left navigation systems and digital controls vulnerable, since altered software or networked boards can, for instance, directly affect ship handling (Kechagias 2022). Offshore energy installations face similar risks, as their increasingly connected industrial control systems are exposed to digital interference (Mohammed 2022).

The growing importance of undersea networks cannot be overstated. Their landing stations and monitoring systems are considered particularly sensitive, as they are indispensable for global data traffic and can themselves

become targets (European Parliament 2022; ENISA 2023). Taken together, these findings show that a wide range of maritime systems face increasingly serious cybersecurity challenges.

Recent Incidents and Windows of Cyber Exploitation

Cable failures are not isolated risks but recurring occurrences. This was 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 temporarily without stable internet and, in some cases, without landline access. The event was described as a "major incident", and restoration took several days (BBC 2022). Multiple fibre cables in southern France were also cut around the same time; 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 a network is already under pressure, it becomes easier to disguise DDoS attacks, routing manipulation such as BGP hijacking is more easily overlooked, and overwhelmed monitoring and incident-response systems react more slowly. Research into the maritime threat landscape shows that attackers exploit these stressful moments to infiltrate malware or gain access to landing 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" vessels systematically survey underwater networks across Europe, including cables, power lines and pipelines. Recent reports point to Russian vessels tracking subsea cable routes and conducting reconnaissance in European waters (DataCenterDynamics 2025; WTOP 2025). Investigations have also revealed Russian naval activity around the Nord Stream explosion sites, pointing to a broader pattern of underwater intelligence activity tied to hybrid operations (Whit 2023).

Several policy analyses suggest Russia increasingly views submarine cables as just another strategic lever, employing covert reconnaissance, prepositioning and plausible sabotage designed to resemble accidents (EPRS 2022; EUISS 2023; Hybrid CoE 2025). Russia conducts reconnaissance of underwater infrastructure through vessels such as the Yantar and is building a growing shadow fleet that blends military operations with civilian cover (EUISS 2023; EPC 2024; Foreign Affairs 2023). Analysts outline scenarios in which Russia deliberately damages individual cables in the North Atlantic or Baltic Sea, exploiting their vulnerability without ever crossing the threshold of open attack, in order to create uncertainty, apply economic

pressure and test NATO's response (Hybrid CoE 2025; NATO Defence College 2023).

This kind of cyber-based prepositioning, meaning the quiet build-up of access to digital control systems, allows attackers to act quickly and with ease should a crisis emerge. Espionage, malware injection and attempts to exploit vulnerabilities in remote access systems are common tactics within ground stations and network operations centres (EPRS 2022; ENISA 2023). Such activity rarely leaves a clear trace and may go undetected for months or even years.

Real-world events underscore how closely physical and digital risks are intertwined. The 2022 Shetland cable outages and the sabotage near Marseille caused regional disruptions and temporarily weakened digital monitoring along the affected routes (NYT 2022; Shetland News 2025; Shetland Times 2025; Heise 2023). Overloaded networks and impaired monitoring systems make it easier to disguise DDoS attacks or route manipulation, an interplay increasingly seen as central to hybrid threats, which tend to prioritise strategic uncertainty over outright destruction (Hybrid CoE 2025; Foreign Affairs 2023). Even a temporary halt to a single transatlantic cable could slow communication between European governments and US military institutions (EPRS 2022; EUISS 2023; Atlantic Council 2024). Combined with disinformation, for example framing sabotage as a "technical error", this can produce an information vacuum that hampers decision-making (Hybrid CoE 2025; Politico 2024; Forbes 2025).

Future threat activity is expected to concentrate in the North Atlantic, North Sea and Baltic Sea, regions marked by high geopolitical tension and dense cable networks (Atlantic Council 2024; EUISS 2023; EPC 2024). While Russia exerts hybrid pressure on Europe, China continues to expand and globalise its network of cables, operators and technology partners (EPRS 2022; Foreign Affairs 2023; EPC 2024). Both trends increase the likelihood that submarine cables will become a new instrument of geopolitical competition for cyber actors (Hybrid CoE 2025; EPRS 2022).

Strengthening Resilience: Priorities for the EU and NATO

Strengthening resilience requires closer integration of maritime surveillance, cybersecurity and international cooperation (EUISS 2023; Hybrid CoE 2025; Atlantic Council 2024). Continuous monitoring of the underwater space is essential, as current systems still leave significant detection gaps (European Union 2025). This includes sensor-based maritime reconnaissance and the integration of satellite and ship-traffic data (Hybrid CoE 2025). Another priority is mandatory cybersecurity standards for landing stations: the EU's Recommendation (EU) 2024/779 sets out minimum requirements for critical infrastructure operators, including tighter access controls, regular security audits and consistent patch management (Commission Recommendation 2024). These standards should be made

compulsory for cable operators and reinforced by joint CERT capacity (Cattler 2024).

Because the security of deep-sea cables is inherently cross-border, the EU and NATO need a unified, permanent system combining maritime situational reports, technical data and cyber threat analysis (Hybrid CoE 2025; Cattler 2024). Europe must also increase redundancy through additional cable routes and alternative landing points. The European Commission warns that too few redundant connections constitute a "structural risk" with "immediate economic consequences" of their own (JRC 2025). Island regions in particular require additional cables or more robust satellite networks.

Deep-sea cables may sit beyond sight, but their protection has become central to European cybersecurity policy.

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