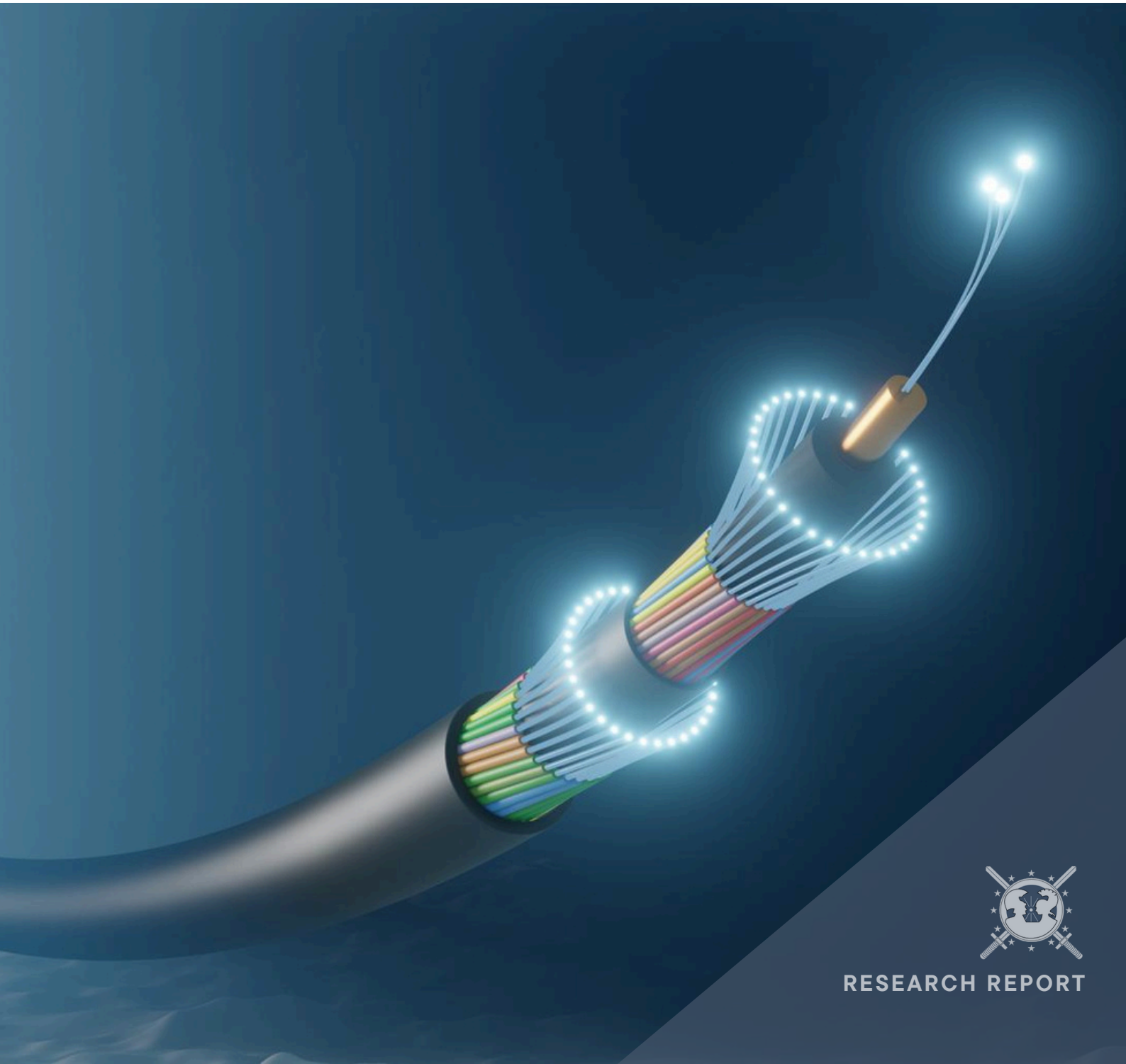
FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

JANUARY 2026

Undersea Warfare in the 21st Century
Part Two: Anti-Submarine Warfare Technology and the Protection of Submarine Data Cables

Rodrigo Andrade Santos
Defence & Security Research Department



RESEARCH REPORT

FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

Defence & Security Research Department

Written by: **Rodrigo Andrade Santos**
Supervised by: **Elise Alsteens & Jennifer Kalushi**
Edited by: **Jackson Elder**

FINABEL's Research Reports are concise, research-driven publications designed to keep Europe's defence community informed about the latest strategic, military, and geopolitical developments. Released three times per week, these short-form papers offer timely analysis on emerging trends affecting European land forces. Each Research Report is produced by the researchers of FINABEL's Permanent Secretariat, in the goal of supporting decision-making across the European defence landscape.

RESEARCH REPORT

Introduction

One of the most critical dimensions of the underwater security sphere is submarine data cables (SDCs). Comprised of more than 500 fibre-optic cables, this network carries 99 per cent of all internet traffic, enabling everything from browsing social media to conducting trillion-euro transactions, transmitting military communication, or carrying sensitive diplomatic cables[1](TeleGeography, 2024; Voce et al., 2025; Ondrášková, 2024; Rossiter, 2025, p.1). SDCs are the basis of global connectivity and the backbone of modern societies. However, because they lie unseen on the ocean floor, these cables have tended to receive little attention from analysts and policymakers until a malfunction or, more critically, an act of sabotage (Bueger 2022, p. 13). Since it is often difficult to assign blame in such events, SDCs make for an increasingly attractive grey-zone warfare target (Bueger & Liebetrau, 2023, p. 5). Recent disruption events attest to this view, requiring modern security assessments to address new threats to submarine cable networks (Pohoryles, 2025, p. 6).

This paper is the second in a two-part series examining contemporary and near-future perspectives on anti-submarine warfare (ASW) doctrine and capabilities. Building on the final section of Part One, Emerging Trends and Capabilities in ASW, it begins by framing SDCs as strategic targets and explores how ASW-related technologies can both protect and threaten undersea cable infrastructure. The paper then reviews current relevant projects and identifies the crucial role of private actors in the loosely regulated SDC landscape.

2. Submarine Cables as an Undersea Warfare Target

Each year, there are over a hundred breaks in SDCs (Eriksud, 2023, p. 1). Most incidents are unintentionally caused by human activity, such as fishing trawlers or anchors (Pohoryles, 2025, p. 6). However, suspicions of deliberate sabotage are becoming more frequent. Analysts and decision-makers are beginning to recognise the vulnerability of SDCs, fuelled by the growing reliance of society on the undersea communication network. The number of SDCs has more than doubled over the last 15 years, and demand for capacity continues to grow at pace (Voce et al., 2025; Rossiter, 2025, pp. 1-2). Technological advances, which are encouraging greater economic exploitation of the undersea domain for both energy and raw materials, are congesting the seabed and heightening the risk of accidentally damaging SDCs (Rossiter, 2025, p. 2; Bueger and Liebetrau, 2023, p. 3). Finally, the 2022 sabotage of the Nord Stream 1 and 2 pipelines widely served as a wake-up call for the need to protect critical undersea infrastructure (CUI). These incidents exposed the inadequacy of existing safeguards and response mechanisms, raising concerns within governments over the security of these 'invisible' undersea assets (Rossiter, 2025, p. 2; Bueger & Liebetrau, 2023, pp. 1, 5).

The lack of adequate security for undersea cables creates avenues for hostile actors to conduct sabotage operations while claiming plausible deniability. Potential saboteurs can employ civilian vessels carrying anchors, fishing gear, and dredging equipment to damage CUI and cause economic, social, and geopolitical turmoil, while remaining below the threshold of open military action (Voce et al., 2025; Joint Research Centre [JRC], 2025; Bueger & Liebetrau, 2023, p. 5). Proving intent to interfere with undersea cables is remarkably difficult, particularly when suspected ships fly 'flags of convenience',[2] complicating the process of

[1] The use of the term 'cable' to refer to diplomatic communication dates to the flow of messages sent through underwater telegraph cables that began to connect nations in the 19th century (Siegel & Raz, 2010). While those cables are long gone, the expression has endured and remains accurate, as modern communications between governments still travel through fibre-optic submarine cables (Ondrášková, 2024).

[2] These are ships whose ownership is registered in countries with looser regulations and greater anonymity, and whose crews are often recruited from multiple countries (Voce et al., 2025).

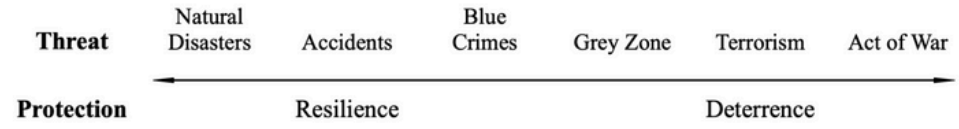
attributing an incident to a primary instigator (e.g. state actor) (Voce et al., 2025; Rizzi & Ogryzko, 2025). Additionally, crews utilising civilian vessels can claim that any damage was accidental. While 20 per cent of known CUI disruptions remains unknown, the expanding pattern of incidents suggests that some may have been intentional (Van Soest, 2025, p. 4; Voce et al., 2025). The attacks on the Nord Stream pipelines are archetypal examples: although the perpetrator remains unknown, the intent is clear, and the incident's high sophistication suggests at least some form of state sponsorship (Bueger & Liebetrau, 2023, p. 5).

In the event of a full-scale war, it is widely acknowledged that militaries would openly target CUI (Rossiter, 2025, p. 1). Isolated disruptions are costly nuisances, but the consequences of a large-scale attack would range from simultaneous outages in essential services to the severing of military communications and intelligence feeds (Rizzi & Ogryzko, 2025; Rossiter, 2025, p. 2). Against a backdrop of escalating geopolitical tensions, recent cable disruptions strengthen the case for bringing SDCs to the forefront of defence and security debates.

3. Anti-Submarine Warfare Technology and the Protection of Submarine Data Cables

As with ASW, existing discussions on the protection of SDCs highlight the potential of emerging undersea technologies, such as unmanned underwater vehicles (UUVs) or big-data analytics, as potential paradigm shifters. However, progress has emerged as a double-edged sword, as advances in undersea capabilities enable actors to target and damage SDCs more effectively. The current threat landscape facing SDCs can be understood as a spectrum ranging from natural disasters to outright acts of war.

Figure 1: Threat and Protection Spectrum for SDCs



Source: adapted from Bueger & Liebetrau (2023)

At the left side of the spectrum in Figure 1, protection efforts emphasise resilience to mitigate potential disruptions to the undersea network. Toward the right side, threats become more consequential, and the focus of protection measures shifts to deterring such events altogether. The following sections examine how emerging ASW-related technologies can be applied to the protection of SDCs, with a particular emphasis on deterring malicious acts, and how their militarisation could, in turn, pose serious threats to this infrastructure.

3.1. *Protection Dimension*

A cable stretching for hundreds or thousands of kilometres is a difficult asset to protect (Eleftherakis & Vicen-Bueno, 2020, p. 34; Prysmian, n.d.). A longstanding practice for safeguarding SDCs in shallower areas is burial, but this technique has proven insufficient in protecting against intentional damage (Pohoryles, 2025; Voce et al., 2025). In waters deeper than 2000 metres, cables lie unburied on the seafloor (JRC, 2025). Surveillance is another common practice employed to protect SDCs. Currently, it relies on general Maritime Domain Awareness (MDA), which depends on the tracking of commercial ships' routes through an

Automatic Identification System (AIS), and is complemented by coastal radars, cameras, and air and seaborne patrols. Next-generation undersea sensors and craft could elevate surveillance capabilities, particularly when threats move underwater, and the likelihood of detection drops sharply (Bueger and Liebetrau, 2023, p. 6).

To address potential undersea threats such as divers, anchors, fishing trawls, or hostile UUVs, Eleftherakis & Vicen-Bueno (2020, p. 27) propose combining sensors with uncrewed vehicles. Militaries could equip undersea drones with existing ASW technology, such as towed arrays, hull-mounted and dipping sonars, or hydrophone systems, or attach scientific devices to the crafts, including seabed mapping systems, turbidity sensors, cameras, and magnetometers (Eleftherakis & Vicen-Bueno, 2020, pp. 27-32). The underlying logic in deploying these UUVs is to achieve deterrence by denial. If an attacker's chances of being detected increase, they are less likely to attempt cable-disruptions (Rossiter, 2025, p. 4). Threats can be spotted early and addressed quickly, whether by preventing sabotage or by conducting rapid repairs to damaged cables. If UUVs develop the capability to restore an undersea cable's functionality swiftly and at low cost, they can diminish the disruptive effects of a potential attack and reduce the incentive for sabotage. Bulky remotely operated vehicles (ROVs)[3] with sensors and robotic arms are already repairing SDCs, albeit with limitations (Rossiter, 2025, p. 4). Overall, UUV improvements in both detection and repairs could simultaneously reinforce deterrence and resilience of undersea networks.

Advances in quantum computing technology will be key in improving the capabilities of UUV-mounted sensors. Quantum computing will accelerate big-data processing, increasing the signal-to-noise ratio and thereby improve the efficiency of sensors (Ondrášková, 2024). Artificial Intelligence (AI) and machine learning (ML) models are transforming telemetry processing and threat anticipation. By combining the three, militaries can better identify undersea environmental conditions, patterns, and suspicious behaviours and enhance their MDA (Telecom Review, 2025; Bueger & Liebetrau, 2023, p. 6). This will strengthen early-warning mechanisms and provide sea-denial effects against hostile actors, improving the cable network's resilience. Additionally, the increased likelihood of detection could deter malicious actors from targeting SDCs.

3.1.1. *Distributed Fibre Optic Sensing*

One notable feature of emerging sensing capabilities is the repurposing of SDCs to not only carry data but also operate as sensors of their surrounding environment (Prysmian, n.d.). This technology, known as Distributed Fibre Optic Sensing (DFOS), comprises three primary modalities. Distributed Acoustic Sensing (DAS) detects vibrations and acoustic signals along a cable, allowing for the detection of nearby disturbances, such as digging, tapping, or water movements. Distributed Temperature Sensing (DTS) monitors temperature changes along the cable, and Distributed Strain Sensing (DSS) identifies structural variations in the fibre, including stretching, bending, or pressure changes. Anomalies in these parameters can determine the location of interferences to cable sections within a few metres, and provide size and trajectory estimates of nearby objects (Prysmian, n.d.). When combined with AIS data, militaries can link the movements of surface

[3] ROVs are one of the two primary types of UUVs. The other are autonomous underwater vehicles (AUVs) (Willett, 2024, p. 1).

ships with, for example, an anchor disturbing the seabed, warning navies and/or coast guards. This DFOS technology can be adapted to existing cables. Signal repeaters (i.e., the 'listening' components) can be installed roughly every 100 kilometres along an existing line, avoiding the prohibitive costs and the logistical burden of laying new cables (Prysmian, n.d.; Abrão, 2025).

3.1.2. *Key Considerations*

As Zaccagnini and Leccese (2025) predict, data collected through fibre-optic sensing, processed with quantum computing and AI, and complemented by other intelligence sources, could guide an integrated system of manned and unmanned fleets capable of better protecting SDCs. This promise of a technological way forward has yet to be fulfilled, and current limitations on UUVs' endurance and onboard sensors' capacities will provide an incomplete picture of the vast seas for some time still. Nonetheless, the growing number of actors acquiring UUVs should come as evidence of a field maturing rapidly, with capacity to level the playing field in terms of affordability (Rossiter, 2025, pp. 3-4). Ownership of these devices has expanded beyond the portfolios of powerful navies, with about fifty states now possessing them. Moreover, their relatively low cost means that non-state actors can acquire them too. For example, in 2021, Hamas used an uncrewed platform in an attempted attack on Israeli offshore energy installations. In 2024, Houthi rebels deployed UUVs against commercial vessels in the Red Sea (Rossiter, 2025, p. 3).

3.2. *Threat Dimension*

While developments in ASW capabilities may equip navies with more adequate technology to defend SDCs, hostile actors can utilise the same technologies to conduct undersea sabotage operations more effectively. Often, the offensive dimensions of these technologies require less effort to employ than the resources necessary to counter them. Just as a submarine enjoys a stealth advantage against detection systems in the vastness of the oceans, a small uncrewed craft targeting one cable segment faces a far easier task than one attempting to defend the entire line. Similarly, producing an effective repair UUV takes longer than building a simple device armed with explosives to damage an SDC. As such, an attacker holds a deployment edge and the first-mover advantage (Rossiter, 2025, p. 4). Certainly, a cable's vulnerability depends on the diving range. Yet, much of the SDCs network lays on shallow waters and can be attained by modest UUVs capable of enduring depths of 3000 metres. A case in point is the shallow seabeds of the Baltic and North Seas – averaging 52 and 95 metres, respectively – which already witness frequent incidents, suggesting how such vulnerabilities could be further exploited by simple unmanned vehicles (Voce et al., 2025; Rizzi and Ogryzko, 2025). As seabed warfare evolves,[4] the whole network of undersea cables, spanning from shores to the deep seafloor, will become targetable, and the areas requiring monitoring will expand accordingly (Willett, 2024, para. 15; Rossiter, 2025, p. 3). Furthermore, as technology advances, the availability of UUVs grows, which in turn heightens the likelihood of man-made threats (see Fig. 1), involving both state and non-state actors (Willett, 2024, para. 6).

Regarding non-physical threats to SDCs, notable examples include decryption and jamming. Tapping of subsea cables is still considered highly unlikely. However, the potential of quantum computing already makes

[4] Some Western navies are soon expected to be capable of conducting seabed warfare at depths of 6,000 metres, which would nearly cover the entire North Atlantic seabed (Willett, 2024, p. 4). In turn, China has recently launched a deep-sea device capable of severing SDCs down to 4000 metres (Hu, 2025).

attempts to access SDC data rewarding, in anticipation of future decryption (Bafoutsou et al., 2023, p. 19; Bryan, 2025). Jamming attacks disturb data transmission by sending a signal into a cable, either increasing the error rate in the incoming data or overloading a receiver. Sensing attacks represent an evolution of conventional jamming attacks, where a wavelength-specific signal is emitted into DFOS-equipped cables, particularly those using DAS, potentially leading to the leakage of what the able detects in its surrounding environment. This technique, known as the Narrowband Jamming Attack (NJA), differs from jamming aimed solely at disrupting communication (a denial-of-service). Instead, it turns a cable's sensing capabilities to the saboteur's advantage. Despite lacking real-world validation, the feasibility of NJA has been confirmed through simulations, highlighting the risks associated with integrating DAS into SDCs (Song et al., 2025, pp. 2-7). Again, protective measures appear to lag behind emerging threats, signalling the need for thorough dialogue across the industry – particularly among major cable investors, who are certainly interested in protecting their assets, but may fear the militarisation of their assets. The likelihood of an SDC being targeted in a conflict increases the more it serves a military purpose. This includes sensing cables, as well as those connecting naval bases and satellite receiving stations (Bueger et al., 2022, p. 23). These considerations underscore the importance of assessing the broader implications of technological advances, rather than focusing on progress in isolation.

4. Existing Projects

Several initiatives have sought to apply ASW principles to SDC defence, typically as part of a comprehensive approach by navies to protect CUI (Van Soest, 2025, p. 4).[5] In 2022, the French Navy launched Operation Calliope to monitor seabeds for hybrid threats. UUVs equipped with sensing capabilities are being developed within this programme, and France is expected to manufacture its own UUVs by 2026 (Willett, 2024, p. 4-6). In 2023, the British Royal Navy launched *Proteus*, a ship fitted with advanced monitoring systems, carrying surveillance and warfare-ready UUVs, operating under the Multi-Role Ocean Surveillance Ship (MROSS) program. In November 2024, *Proteus* was dispatched to monitor Russia's *Yantar* ship amid suspicions of surveillance operations in British waters (Royal Navy, 2023; Willet, 2024, p. 8; Voce et al., 2025).

However, given the cross-border nature of CUI, nations must cooperate to address their security and defence. In 2022, following the Nord Stream incidents, NATO established the Critical Undersea Coordination Cell, mobilising states, partners, and companies towards this goal (Voce et al., 2025). In 2023, the EU's Permanent Structured Cooperation (PESCO) established the Critical Seabed Infrastructure Protection (CSIP) project, which, through UUVs, aims to shield structures like SDCs from sabotage and natural events (Permanent Structured Cooperation [PESCO], 2023). Within the framework of the European Defence Fund, the 2024-2028 SEACURE project is assembling European private entities to develop an integrated system-of-systems for uncrewed anti-submarine and seabed warfare operations, including the defence of CUI (European Commission, 2024). In January 2025, the Joint Expeditionary Force [6] activated Nordic Warden, initiating joint patrols and data sharing through an AI-based response system to address threats against undersea cables (Zaccagnini & Leccese, 2025; Van Soest, 2025, p. 4). NATO followed with Baltic Sentry, aiming to increase the monitoring of critical seabed infrastructure through the coordinated use

[5] Several programs and directives, such as the EU's Network and Information Security Directive 2 (NIS2) on cybersecurity and the Critical Entities Resilience Directive (CER), address the securitisation of SDCs. However, despite their relevance for the complete picture of cable's protection mechanisms, they fall outside the link between military thinking and the defence of SDCs that guides this paper (Pohoryles, 2025, p. 4).

[6] Composed by Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, the Netherlands, Norway, Sweden, and the United Kingdom (Van Soest, 2025, p. 4)

of manned and unmanned units (Zaccagnini & Leccese, 2025). Admiral Giuseppe Dragone, the chair of NATO's Military Committee, pointed to the absence of incidents in 2025, in contrast to 2023 and 2024, as evidence of the operation's success as a deterrent (Milne, 2025, p. 3). Finally, in February 2025, the European Commission launched the EU Action Plan on Cable Security, calling for the adoption of Science Monitoring and Reliable Telecommunications (SMART) cables. Although designed for environmental studies, the plan is also envisioned for military purposes through DFOS (Zaccagnini & Leccese, 2025). SMART cables, however, are a paradigmatic example of the barriers involved in translating military ASW approaches to civilian-oriented infrastructures, such as SDCs. So far, the InSEA Wet Demo is the project's only operational cable, located off the coast of Sicily (Calver et al., 2025; SMART Cables, n.d.). Remaining plans have mainly been restricted to intrastate projects,[7] as fear over improper data gathering have sparked national security concerns (Zaccagnini & Leccese, 2025).

These projects reveal growing recognition of the critical nature of SDCs. While positive, these efforts have led to a proliferation of fragmented initiatives, often overemphasising military responses and overlooking the intricacies of undersea cable networks. In the long term, such an approach is unsustainable and highlights the need for coordinated stakeholder efforts to protect this vital asset (Van Soest, 2025, p. 5).

5. The Private Sector and the Regulatory Gap

Any analysis of undersea cables is incomplete without an understanding of their complex ownership structures and the relatively limited regulatory framework governing them. SDCs are mainly owned by an international consortium of telecoms and big tech firms, as they possess a direct interest and capacity for such substantial investments (Jeon & Rysman, 2024, p. 6; Saunavaara & Salminen, 2023, p. 8).[8] Thus, these firms largely dictate the terms of cable installations (i.e., routing) and respective data flows (Saunavaara & Salminen, 2023, p. 8). Additionally, they possess expertise on the functioning, maintenance, and vulnerabilities of these structures. States have delegated control over this critical infrastructure to such an extent that private companies now serve as inevitable intermediaries in SDC debates and, to some degree, as arbiters of state power (Ganz et al., 2024, pp. 5-6). Worryingly, as their security priorities may diverge, governments may struggle to leverage or secure SDCs in accordance with national strategies. Moreover, few governments have developed regulatory frameworks reflecting the importance of these systems (Ganz et al., 2024, p. 3; Rossiter, 2023). This can be partly due to the borderless nature of the high seas, which complicates the legal status of cables (Ganz et al., 2024, pp. 4-5). Lacking national affiliation, a cable is regulated differently by each jurisdiction it traverses, with the broad United Nations Convention on the Law of the Sea (UNCLOS) serving as the closest comprehensive framework[9](Ganz et al., 2024, p. 4; Saunavaara & Salminen, 2023, p. 5).

[7] Among the three launched projects, including the InSEA Wet Demo, only one, connecting Vanuatu and New Caledonia, crosses territorial seas. Of the cables currently 'in planning,' only four out of eight envisage connecting different nations (SMART Cables, n.d.).

[8] Since 2016, overwhelming investment by big tech firms and content providers has seen these actors shift from being capacity buyers to major cable developers, transforming cable-laying dynamics and ownership models. Currently, Meta, Google, Microsoft, and Amazon have a substantial ownership share of the submarine cable network (Jeon & Rysman, 2024, p. 6; Saunavaara & Salminen, 2023, p. 8). These content providers, also known as 'hyperscalers' (Gjesvik, 2023, p. 723), sought to have more control over the terms on which their data flows to optimise the delivery of their product (Jeon & Rysman, 2024, p. 6).

[9] The 1982 UNCLOS is the predominant international treaty governing the rights of installation and protection of SDCs, and it ratifies a country's ability to develop its own regulation on submarine cables in its territorial waters and asserts the right of any country to establish submarine cables beyond those boundaries (Ganz et al., 2024, p. 4; Rossiter, 2023; Saunavaara & Salminen, 2023, p. 5).

Private actors bridge the military-civil divide and have a responsibility to contribute to undersea infrastructure security efforts, if only to protect their assets. Private-public partnerships between corporations and militaries provide a promising route forward for the protection of CUI. In 2021, the United States established the Cable Security Fleet, comprising private vessels contracted to provide repairs upon request for undersea cables (Rossiter, 2025, p. 2). In the same year, the Norwegian Navy investigated the severing of a Lofoten–Vesterålen (LoVe) cable using UUVs sourced from the oil and gas sector (Berglund, 2021; Willett, 2025). Data from the LoVe sensing cables is reportedly shared with the Norwegian Ministry of Defence in yet another sign of a close and effective civil–military collaboration on CUI security, in the country (Willett, 2024, p. 4; Willett, 2025). Similarly, in 2022, the Italian Navy reached an agreement with Sparkle, offering better protection for the company's cables in return for access to their location and sensing data (Kington, 2022).

Governments and private actors must collaborate to advance the securitisation of SDCs. Coordination is easier within territorial waters, and some governments have already established protection zones for private undersea cables (Rossiter, 2025, p. 2). Matters become more complex, however, when a cable reaches the high seas. The challenge lies in achieving operational interoperability among all parties to protect SDCs and agree on cost-sharing. Regarding sovereignty, the issue extends to whether one state would allow another to operate sensors and UUVs within its territorial waters. High cable density adds another layer of complexity, particularly near sites where undersea cables make landfall, as efforts to protect individual cables risk encroaching on neighbouring systems or triggering eavesdropping suspicions. Sovereignty concerns surrounding sensing cables may lead states to invoke national security or improper data collection of their marine environment, highlighting the barriers that can be erected against private initiatives and/or transnational sensing cables (Zaccagnini and Leccese, 2025, paras. 3-4). From a threat perspective, the interconnected nature of SDCs means that attacking a 'foreign' cable risks crippling the attacker's own communications and internet, resulting in a deterrence logic anchored on mutual cable dependence.

Conclusion

The criticality of SDCs is as great as their vulnerability. While developments in drone technology, big-data analytics, and DFOS may help create a more resilient undersea network, hostile actors can exploit these capabilities to target the vast SDC network. While protection initiatives are already underway, efforts are fragmented and risk over-militarising what is predominantly civil-oriented infrastructure. In addition, any defence strategy cannot circumvent the central role of private companies as the primary owners of SDCs. Therefore, securing this vital network will require bridging the civil-military divide and bringing all stakeholders to the table to develop interoperable practices that protect this increasingly targeted asset amid intensifying hybrid threats.

Bibliography

Abrão, G. B. (2025). Nova tecnologia em cabos submarinos pode detectar sabotagem e ser instalada em linhas já existentes. *Mundo Conectado*. https://www.mundoconectado.com.br/internet/nova-tecnologia-cabos-submarinos-com-sonar-anti-sabotagem/

Bafoutsou, G., Papaphilippou, M., Dekker, M., & ENISA. (2023). Subsea cables: What is at stake? *European Union Agency for Cybersecurity (ENISA)*. https://data.europa.eu/doi/10.2824/212261

Berglund, N. (2021, November 7). Surveillance cables mysteriously cut. *Norway's News in English*. https://www.newsinenglish.no/2021/11/07/surveillance-cables-mysteriously-cut/

Bryan, G. (2025). *Cybersecurity Challenges in Submarine Cable Systems*. TeleGeography. https://blog.telegeography.com/cybersecurity-submarine-cable-systems

Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy*, *155*, 105772. https://doi.org/10.1016/j.marpol.2023.105772

Bueger, C., Liebetrau, T., & Franken, J. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. *Policy Department for External Relations Directorate General for External Policies of the Union*. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Calver, J., Watkiss, N., Restelli, F., Kerkenyakova, A., & Mohr, S. (2025). *Successful Deployment of a 21km SMART Cable with Force-Feedback Seismometer and Accelerometers in the Mediterranean Sea* (Nos EGU25-16799). EGU25. Copernicus Meetings. https://doi.org/10.5194/egusphere-egu25-16799

Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors. *Sensors (Basel, Switzerland)*, *20*(3), 737. https://doi.org/10.3390/s20030737

Eriksrud, M. (2023). Protecting submarine cables for enhanced connectivity. *Open Access Government*, *38*(1), 442–443. https://doi.org/10.56367/OAG-038-10729

European Commission. (2024). SEACURE - Seabed and Anti-submarine warfare Capability through Unmanned feature for Europe. European Union. https://defence-industry-space.ec.europa.eu/document/download/32604a9c-bffa-48ce-905e-86b320b81446_en?filename=EDF-2023-DA-UWW-ASW%20SEACURE.pdf

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

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. Review of International Political Economy, 30(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Hu, B. (2025). China Discloses Powerful Deep-Sea Cable Cutter, SCMP Reports. Bloomberg.Com. https://www.bloomberg.com/news/articles/2025-03-22/china-discloses-powerful-deep-sea-cable-cutter-scmp-reports

Jeon, J. & Rysman, M. (2024). Investment and Usage of the Subsea Internet Cable Network. Proceedings of the TPRC2024 The Research Conference on Communications, Information and Internet Policy. https://ssrn.com/abstract=4925783

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

Kaushal, S. (2025). Anti-submarine warfare: A scalable approach. ESD. https://euro-sd.com/2025/03/articles/43257/anti-submarine-warfare-a-scalable-approach/

Kington, T. (2022, July 14). Italian Navy, telecom provider team up to deter attacks on undersea cables. Defense News. https://www.defensenews.com/naval/2022/07/14/italian-navy-telecom-provider-team-up-to-deter-attacks-on-undersea-cables/

Milne, R. (2025). Nato considers being 'more aggressive' against Russia's hybrid warfare. *Financial Times*. https://www.ft.com/content/dbd93caa-3c62-48bb-9eba-08c25f31ab02

Ondrášková, J. (2024). Securing Our Digital Lifelines: Quantum Technology and the Battle for Arctic Supremacy. The Arctic Institute - Center for Circumpolar Security Studies. https://www.thearcticinstitute.org/securing-digital-lifelines-quantum-technology-battle-arctic-supremacy/

Permanent Structured Cooperation. (2023). Critical Seabed Infrastructure Protection (CSIP). https://www.pesco.europa.eu/project/critical-seabed-infrastructure-protection-csip/

Pohoryles, D. (2025). Risks and protection of subsea cable networks. Publications Office of the European Union, JRC142001. https://doi.org/10.2760/0196933%2520(online)

Prysmian. (n.d.). Subsea cables as sabotage sensors and environmental monitors | Prysmian. Prysmian Magazine. https://www.prysmian.com/en/insight/nexst/digital-solutions/subsea-cables-as-sabotage-sensors-and-environmental-monitors

Rizzi, A., & Ogryzko, L. (2025). Shallow seas and "shadow fleets": Europe's undersea infrastructure is dangerously vulnerable. European Council on Foreign Relations (ECFR). https://ecfr.eu/article/shallow-seas-and-shadow-fleets-europes-undersea-infrastructure-is-dangerously-vulnerable/

Rossiter, A. (2023). Undersea cables in an age of geopolitical competition. TRENDS Research & Advisory. https://trendsresearch.org/insight/undersea-cables-in-an-age-of-geopolitical-competition/

Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). Marine Policy, 171, 106434. https://doi.org/10.1016/j.marpol.2024.106434

Royal Navy. (2023, January 19). Navy's new guardian of key underwater infrastructure arrives in UK. Royal Navy News / Equipment and Tech. https://www.royalnavy.mod.uk/news/2023/january/19/20230119-navys-new-guardian-of-key-underwater-infrastructure-arrives-in-uk

Saunavaara, J., & Salminen, M. (2023). Geography of the Global Submarine Fiber-Optic Cable Network: The Case for Arctic Ocean Solutions. Geographical Review, 113(1), 1–19. https://doi.org/10.1080/00167428.2020.1773266

Siegel, R., & Raz, G. (Directors). (2010). The History Of The Term ‘Cable’ [Broadcast]. In All Things Considered. NPR. https://www.npr.org/2010/11/30/131704392/the-history-of-the-term-cable

SMART Cables. (n.d.). SMART Systems. SMART Cables. https://www.smartcables.org/systems

Song, H., Chen, X., Gao, J., Yang, T., Xi, J., Zhu, X., Sun, S., Yu, W., Bai, X., Wu, C., & Wei, C. (2025). The Sensing Attack: Mechanism and Deployment in Submarine Cable Systems. Photonics, 12(10), 976. https://doi.org/10.3390/photonics12100976

Telecom Review. (2025). Safeguarding Submarine Cables in the AI Era. Subsea Cables by Telecom Review. https://www.subseacables.net/reports-and-coverage/safeguarding-submarine-cables-in-the-ai-era/

TeleGeography. (2024). Transport Networks Executive Summary. https://www2.telegeography.com/download-transport-networks-research-service-executive-summary

Van Soest, H. (2025). Protecting Europe’s Critical Undersea Infrastructure Depends on Coordination and Collaboration. RAND. https://www.rand.org/pubs/commentary/2025/06/protecting-europes-critical-undersea-infrastructure.html

Voce, A., Ahmedzade, T., & Kirk, A. (2025). ‘Shadow fleets’ and subaquatic sabotage: Are Europe’s undersea internet cables under attack? The Guardian. https://www.theguardian.com/world/ng-interactive/2025/mar/05/shadow-fleets-subaquatic-sabotage-europe-undersea-internet-cables-under-attack

Willett, Dr. L. (2024). AUVs and ROVs make key contribution to seabed warfare. European Security & Defence. https://euro-sd.com/2024/04/news/37514/auvs-and-rovs-make-key-contribution-to-seabed-warfare/

Willett, L. (2025). Critical undersea infrastructure protection: An interview with Rear Admiral Oliver Berdal, Chief of the Royal Norwegian Navy. Ocean Robotics Planet Magazine, (Special Report), 40–42. https://www.rovplanet.com/tportal_upload/md_publications/rovplanet_202501.pdf

Zaccagnini, I., & Leccese, G. (2025). Securing the Depths: Rethinking EU Critical Infrastructure Protection in a Contested Underwater Domain. CSDS. https://csds.vub.be/publication/securing-the-depths-rethinking-eu-critical-infrastructure-protection-in-a-contested-underwater-domain/

F I N A B E L

THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION