The Sea's Signature: Turning Oceanographic Data into Intelligence for Underwater Infrastructure Security

Giacomo Leccese

LUISS Guido Carli University, Italy

Abstract

The protection of European critical undersea infrastructure has become a central security priority following recent sabotage and the growing recognition that underwater energy and communication flows are particularly exposed to hybrid threats. The maritime and especially the underwater environment limits sensor coverage, constrains communication, and intersects with multiple jurisdictions, complicating intelligence collection. As European institutions and NATO have begun exploring ways to enhance maritime situational awareness, growing attention has been directed toward the potential contribution of civilian oceanographic sensors, whose data are routinely collected for scientific research or infrastructure monitoring. Yet, despite extensive policy interest, their concrete value for intelligence collection remains under-examined.

The article addresses this gap by asking how and to what extent civilian oceanographic sensors can support intelligence collection against hybrid threats to critical undersea infrastructure. Building on literature on Geophysical Measurement and Signature Intelligence (MASINT) and the challenges that hybrid threats pose to intelligence collection, the paper advances the argument that civilian oceanographic sensors can provide meaningful, albeit not comprehensive, support across three core functions: detection, attribution, and the facilitation of intelligence sharing.

Methodologically, the article employs counterfactual analysis to study how the presence of this new variable, the use of civilian oceanographic sensors, could have influenced past or hypothetical cases

of sabotage. The three case studies examined are chosen on the basis of the three main threats towards underwater infrastructures identified in the literature: the weaponization of civilian vessels; underwater interference conducted by divers, submarines, or unmanned vehicles; and cyberattacks.

Across these cases, the findings show that civilian sensors offer the strongest contribution to detection and warning, especially through the identification of acoustic and pressure anomalies in the vicinity of infrastructure. Their role in facilitating intelligence sharing is equally significant, since unclassified data can complement sensitive military sources and reduce long-standing barriers to international and interinstitutional cooperation. Their contribution to attribution, while more limited, remains relevant for technical reconstruction and for the identification of attack vectors, though they do not meet the evidentiary requirements for political and legal attribution.

Overall, the article provides the first systematic assessment of the potential and limits of civilian oceanographic sensors for the protection of critical undersea infrastructure. It also identifies several lines for future research that are essential for advancing the study of civilian sensing in underwater security. First, a more fine-grained assessment of detection ranges, environmental constraints, and response times is needed to evaluate the warning value of these sensors under varying oceanographic conditions. Second, further work should examine the legal mechanisms that govern the use of classified information in judicial processes, and how these interact with the growing availability of unclassified civilian data. Finally, the regulatory and organisational frameworks that structure the circulation of data collected by private operators require deeper analysis, particularly given their centrality in any future European model of shared maritime situational awareness.

Introduction

Since the sabotage of the Nord Stream gas pipeline in September 2022, the security of European critical undersea infrastructure (CUI) has become a central topic. Subsequent damage to various infrastructures, especially in the Baltic Sea but also in other European waters, has demonstrated that this type of infrastructure is particularly exposed to hybrid threats (Humpert, 2022). The maritime environment, and the underwater one in particular, favours this type of hostile activity, which by definition exploits the threshold between detection and attribution, as well as the different interfaces between war and peace, internal and external security, local and state, and national and international (Hybrid CoE, n.d.). In particular, hybrid threats to CUI pose complex challenges for intelligence collection since they occur in a vast, sensor- and communication-averse domain that crosses multiple jurisdictions. Given the need for more data useful for detecting, warning, and attributing potential hostile actions, European states and institutions have explored various solutions aimed at increasing maritime situational awareness. Beyond military patrol of CUI routes, great emphasis has been placed on the potential role of private entities and their sensor capabilities. The EU Action Plan on Cable Security has promoted the use of civilian sensors such as SMART Cables for early warning (European Commission, 2025). NATO has created a Critical Undersea Infrastructure Coordination Cell to facilitate engagement with industry and civilian stakeholders (NATO, 2023). Overall, several analyses emphasize the need to integrate military sensor capabilities with civilian ones, both scientific and from the infrastructure industry (Van Soest, 2025; Bueger & Liebetrau, 2023; Besch & Brown, 2024). However, except for a few studies on the potential use of satellite data, no detailed analysis has been made of how data collected by civilian sensors can contribute to better

protecting CUI and what benefits they could bring (Hendricks & Halem, 2024). How and to what extent can civilian sensors be used to collect intelligence and counter underwater hybrid threats?[1]

This article aims to answer this question, focusing on oceanographic data collected by civilian underwater sensors. These data, closely linked to the scientific dimension, are utilized by both oceanographic research and the infrastructure industry to monitor the underwater environment. In addition to exploring a particularly relevant topic for European security, the article addresses two important gaps in the intelligence literature. First, it analyses the role of Measurement and Signature Intelligence (MASINT) in the protection of critical infrastructure. Second, it explores the civilian dimension of MASINT, which has so far been overlooked in favour of the military one. The article is organized as follows. The first section contains a literature review on geophysical MASINT and the role of oceanographic data in intelligence. The second reconstructs the main challenges posed by hybrid threats to intelligence collection, especially regarding the security of CUI, to create a theoretical framework for analysing and hypothesizing the potential role of civilian oceanographic sensors. The third details the research design. The following sections focus on the empirical analysis, while the conclusions summarize the findings and identify limitations and possible avenues for research.

Literature Review

The collection of oceanographic data is part of the intelligence collection discipline known as Measurement and Signature Intelligence (MASINT). It is defined by Morris as a "technically derived intelligence that detects, locates, tracks, identifies, and describes the specific signatures of fixed and dynamic target sources" (Morris, 1996). Among all the intelligence collection disciplines that have

[1] Intelligence collection can mean both the entire process, from the planning stage to the dissemination of raw intelligence, and a step in the intelligence process in which information or something else of intelligence value is physically acquired (Clark, 2013). This article refers to the second meaning.

joined HUMINT (human intelligence) with technological progress, MASINT is considered the "INT" of science due to the highly technical and scientific means used to develop signatures (National MASINT Office, 2022).

In particular, the collection of oceanographic data falls within the sub-discipline of geophysical MASINT. It entails the collection of physical phenomena of the Earth: energy and disturbances that affect the ionosphere, atmosphere, oceans, solid surface, crust and sub-crust (*Ibid*.). Geophysical MASINT, especially acoustic, is fundamental in the underwater environment. Traditional surface sensing methods, such as radar or imaging, do not work underwater due to physical and environmental phenomena such as the attenuation of electromagnetic waves and light, water turbidity, currents, and sedimentation (Pachaiyappan et al. 2024). The primary tool for detecting submerged objects and underwater activity is sonar, which exploits the greater propagation of sound waves in water compared to air (Waite, 2001). For this reason, the collection of acoustic data has always been considered crucial in antisubmarine warfare (ASW), aimed at detecting, tracking, identifying and engaging enemy submarines.[2]

Despite the established centrality of geophysical MASINT in the underwater environment, I argue that the intelligence literature presents two major gaps, particularly relevant in light of modern threats. First, although geophysical MASINT has been widely studied in the ASW context, the relevance of oceanographic data for protecting CUI has never been analyzed. Critical infrastructure protection does not fall within the fields identified in the literature as the primary application of this intelligence collection discipline (Morris & Clark, 2015). Generally, MASINT is considered very useful

[2] In the Second World War, greater knowledge of the acoustics of the Atlantic gave the German submarine fleet a major advantage. Learning from this, during the Cold War, the US Navy invested large resources in installing the underwater hydrophone network SOSUS (Sound Surveillance System), which was crucial in detecting, tracking, and identifying Soviet submarines (Taddiken & Krock 2021). Even today, ASW relies heavily on acoustic detection, and the underwater traditional hinder-finder competition continues to develop across the acoustic spectrum, exploiting various related oceanographic data such as temperature, salinity and pressure, which influence the sound propagation underwater (Coté Jr., 2012; Gilli et al, 2024)

for situational awareness, but the focus seems to remain on missile, biological, chemical, and environmental threats (*Ibid.*). Conversely, nothing has been written about its potential role in protecting infrastructure. Especially in the underwater environment, where other surveillance methods cannot function, there is a strong need to analyze how geophysical MASINT can contribute to protecting energy and data flows on the seabed.

Second, the literature generally considers MASINT a classified technical intelligence collection since the focus is placed on military sensors (Wolfberg, 2024). In contrast, MASINT, especially oceanographic data that could be useful for understanding the spectrum of underwater threats, is also increasingly collected by civilian sensors. Civilian systems are becoming more common as scientists and governments increase monitoring and management of undersea resources for scientific and economic purposes.[3] In addition to an increasing number of civilian hydrophones used for scientific research, technological progress has also opened the possibility of various fixed or mobile sensing devices used by private companies to monitor the surroundings of their underwater infrastructure. Among these, SMART cables, fiber optic sensing, and the use of underwater drones expand the range of possibilities for gathering underwater intelligence.[4] The data collected by these civilian sensors allows for unclassified MASINT that can be categorized in what the intelligence literature identifies as "publicly" and "non-publicly" available information.[5] As underlined by Clark

[3] Acoustic data is the most exemplary area. Historically, concerns about national security have kept much of this data classified or difficult to access. For years, most non-military hydrophones, except those used to monitor potential nuclear explosions, were deployed for only a few months or years for specific, stakeholder-driven research or monitoring purposes. This changed in 2011, when an international group of experts, concerned with ocean sound and its effects on marine life, began developing the International Quiet Ocean Experiment (IQOE), which encouraged the deployment of civilian hydrophones worldwide. Consequently, the number of hydrophones operating in Europe, North America, and other locations for both research and operational purposes has increased dramatically (Tyack et al., 2021).

[4] These new civil technologies will be explained in detail later in the article.

[5] Publicly available information is unclassified and defined as “information that has been published or broadcast for public consumption, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, or is obtained by visiting any place or attending any event that is open to the public”. There are examples of unclassified data which are not publicly available, yet they may be desired and can be accessed by intelligence agencies by lawful, authorized means. If unclassified information is only available to the intelligence community, and not the public, then it is non-publicly available data (Wolfberg, 2024).

(2015), “an undersea warfare approach will have to take account of this new form of undersea 'encroachment,' especially in terms of inadvertent detection by non-military sensors and protection of friendly infrastructure […]”.

In addition to these two gaps in the intelligence studies, the literature on critical infrastructure protection also presents a fundamental lacuna. Several contributions emphasize the necessary role of private sensors in collecting data essential for seabed protection, but no one has specifically analyzed how such data could help counter hybrid threats (Van Soest, 2025; Bueger & Liebetrau, 2023; Besch & Brown, 2024). The role of civilian sensors is emphasized primarily from a policy-oriented perspective as a recommendation to involve private actors more closely, but how can the data collected by these sensors help intelligence collection? To what extent would they contribute to countering hybrid threats?

Intelligence Collection in the Age of Hybrid Threats: Warning, Attribution and Integration Needs

I aim to create a theoretical framework to analyze how and to what extent civilian oceanographic sensors can be used for intelligence collection to protect CUI against hybrid threats. To do so, I begin by analyzing the main intelligence challenges posed by this type of threat, specifically in the case of CUI. I then hypothesize how civilian oceanographic sensors could fit into this context.

By their very definition, hybrid threats are malign activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international (Hybrid CoE, n.d.). These three features, detection, attribution and complexity, pose significant challenges from an intelligence perspective.

First, a substantial constraint to detection is the combination of military and non-military means. Traditional practices in warning intelligence are biased towards monitoring and assessing previously known conventional (mainly military) capabilities and detecting changes in their posture and

composition, to predict hostile actions from adversaries (Nilsson et al. 2025). Given the modern breadth and ambiguity of possible means of attack, intelligence systems should instead be capable of detecting previously unknown or unanticipated threats as well as previously unseen combinations of threats (*Ibid.*). As underlined by Nilsson et al. (2025), this requires an extensive variety of sensors and capacity for aggregation. When it comes to the security of CUI, the range of threats extends not only from military platforms, such as submarines and uncrewed underwater vessels (UUVs), but also from civilian vessels capable of damaging installations by dragging their anchors, as well as cyber-attacks on the digital systems that regulate the operation of the infrastructure (Bueger et al., 2022).

Second, the ambiguous nature of hybrid threats complicates the collection of intelligence useful for attribution. Intelligence plays a key role in "technical" attribution, which aims to understand how and by whom a hostile action was perpetrated, but it is increasingly called upon to assume a supporting role in "political" and "legal" attribution as well (Council of the European Union, 2022; European Commission, 2024). Even in this case, the traditional intelligence collection system reveals gaps. Aside from insufficient information, attribution is hampered by the fact that data from military sensors cannot be disclosed to develop an evidence base for the public domain (Hendricks & Halem, 2024). When evidence of the activity is based on classified information, public and open evidence-based attribution becomes virtually impossible, clearly favoring the actor behind the activity (Giannopoulos et al. 2021). In the case of sabotage against CUI, European investigators and prosecutors have shown great difficulty in meeting the high bar for criminal evidence of their judicial systems and the requirement of international law to attribute a hostile act to another state (Pancevski, 2024). Yet, for a correct legal attribution, it is necessary to have both evidence that the state "caused" the act and that it was an act by the state or a state organ, or "an entity that the state or its organs exercised effective control over" (Davenport, 2023). In this regard, the widespread

involvement of civilian vessels and the inability to provide supporting evidence based on unclassified information constitute significant obstacles (*Ibid.*).

Third, the complexity of hybrid threats, given the blurring lines between military-civilian, local-national, and national-international, constitutes a further obstacle. As evidenced by Nilsson et al. (2025), "detecting synchronized, multi-vector hybrid attacks intentionally designed to fall outside and/or below traditional detection thresholds requires extensive coordination regarding information sharing". Due to the wide spectrum of vulnerabilities to be monitored and the variety of assets that may be combined to exploit them, effective intelligence assessment depends on the systematic integration of information from multiple intelligence agencies and other intelligence-collector actors to ensure a resilient early-warning and response capability (*Ibid.*). This need for integration exposes another limitation of the current intelligence system. Yet, issues of trust and the exchange of classified information are still difficult to overcome, even among historical allies (Lasoen, 2022). These challenges are particularly significant in the case of the security of CUI. First, these installations often transcend national borders and travel routes that affect multiple national jurisdictions. Second, states have historically been very cautious about sharing data and technologies in the underwater domain (Singh, 2023; Cannon & Bhaat, 2024). Third, especially within the EU framework, a relatively new actor in addressing defense and security issues, member states are reluctant to share details about their critical infrastructure with each other (Besch & Brown, 2024).

I argue that civilian oceanographic data can help overcome the three obstacles just analyzed, even with some limitations. Specifically, I hypothesize that:

1) Civilian oceanographic data can improve detection and early warning by integrating data from military sensors. The literature acknowledges the effectiveness of MASINT in enhancing situational awareness and providing early warning (Morris & Clark, 2015). Given the vastness of maritime spaces, the length of CUI routes, and the high number of potential threats, I

expect that military sensors alone will not be sufficient for adequate maritime situational awareness. In this sense, data from civilian sensors can help detect suspicious activity near infrastructure and preemptively alert authorities, achieving the variety and integration of sensors required by modern intelligence systems to counter hybrid threats (Nilsson et al., 2025).

2) Publicly and non-publicly available intelligence from civilian sensors can partially ease the attribution of an attack, especially in identifying the attacker. This hypothesis is supported by the very nature of MASINT, which is based on "measuring a characteristic of a target (e.g., radiation, vibration, etc.) and then comparing that known characteristic to a library of signatures, which allows a target to be identified and further described" (Sislin, 2019). The identification of the attack vector through civilian sensors can serve both technical attribution, integrating military sensor capabilities, but also political one, allowing the use of unclassified data that can be presented as public evidence. As for legal attribution, I expect civilian sensors to play a lesser role, given that oceanographic data cannot help link an action by a vessel to the intent of a state, unless it is a military vessel. In that case, identifying the attack vector would require matching the signature collected by civilian sensors with one contained in naval intelligence libraries. Such information would be very difficult to present to the public.

3) The less sensitive nature of scientific and industry data can facilitate the exchange of information between allies. While states currently remain skeptical about sharing classified information, this reticence should diminish when it comes to unclassified intelligence. As Corbett and Danoy (2022) emphasize, the availability of high-quality commercial sensors and the growing capabilities for processing and filtering data expand the possibilities for using publicly available information and commercially available information to share intelligence

with allies. This unclassified data facilitates intelligence sharing without compromising sources and methods (Hanna et al., 2017).[6]

Research Design

I test these theoretically-driven hypotheses to analyze how and to what extent civilian oceanographic sensors can be used in intelligence collection aimed at protecting CUI. By civilian oceanographic sensor (independent variable), I refer to sensors used by the scientific community or by companies that own or operate underwater infrastructure. Specifically, the article considers: civilian hydrophones deployed for scientific research; SMART cables, which are temperature, pressure, and acceleration sensors added to repeaters placed along a cable; fiber optic sensing, in which the fiber in the cable is used as a detection tool to statistically categorize frequencies of acoustic noise or other vibration sources; and autonomous underwater vehicles (AUVs) that monitor the surrounding of underwater infrastructure by carrying hydrophones or other types of sensors (Clare, 2022a; Clare 2022b; Clare 2024). The protection of CUI (dependent variable) is conceptualized in terms of both denial, based on the ability to prevent attackers from damaging the infrastructure, and attribution capability.[7] The underwater infrastructures considered will be both energy (pipelines and power cables) and communications (fiber optic internet cables).

To examine the relationship between the dependent and independent variables, the article employs counterfactual analysis, which allows for assessing how the outcome of a past case might have changed if a specific variable had been present or absent. The literature has confirmed the applicability and usefulness of this methodology in political science and particularly in security

[6] For example, data from commercial satellites helped the Quad (United States, Australia, Japan, and India) track Chinese maritime smuggling and maritime militias, and unclassified information provided by the United States to India under a geospatial intelligence cooperation agreement helped Indian forces repel a Chinese incursion along the Himalayan border (Byman, 2025)

[7] The latter perspective refers to the concept of "deterrence by attribution", according to which an adversary can be deterred if it perceives that it will not be able to escape responsibility for an attack (Siman, 2023; Stone, 2021)

studies (Fearon, 1991; Ned Lebow, 2015). By introducing the use of civilian oceanographic sensors into past or hypothetical case, it is possible to evaluate their potential contribution to detection, attribution and information sharing while keeping all other conditions constant. The hypotheses are tested on three case studies: weaponization of civilian vessels; underwater interference via submarines, drones, or divers; and cyberattacks. These cases represent the main threat categories identified in the literature and vary in technological complexity, methods, and attribution challenges, enabling the analysis of threats from the surface, seabed, and land (Bueger et al. 2022; Wall & Morcos, 2022).

The analysis draws on primary and secondary sources, such as academic publications, government, institutional, and industry reports, as well as public interviews with technicians, military personnel, decision makers, and legal experts.

Weaponization of Civilian Vessels

The technologically easiest method to sabotage CUI is through anchor dragging. A commercial vessel can deliberately drag its anchor along the seabed to cut cables and pipelines in waters up to 200 m deep (Eleftherakis & Vicen Bueno, 2020). At least eleven undersea infrastructures in the Baltic Sea have been damaged since October 2023, and the cause has generally been attributed to anchor dragging by commercial vessels (Leicester & Burrows, 2025). Similar suspicious incidents have also occurred outside European waters, such as in the Taiwan Strait (Hioe, 2025).

Detection and warning

The most relevant methods to detect and/or track surface vessels are Automatic Identification System (AIS) data, radar systems, and satellite imagery. AIS data is not a definitive solution since, in several cases, the vessels involved in accidents with the CUI had turned off their transponder (Hioe, 2025). Radar systems and satellite imagery are well-suited for scanning large areas with high spatial

resolution at relatively low cost, but they can only collect imagery intermittently, not allowing continuous monitoring (Paap et al., 2025). Furthermore, radar and satellite cannot sense possible maritime activity below the sea surface close to infrastructure (*Ibid*.). Several European navies have launched patrol and monitoring missions, employing both crewed and uncrewed surface and underwater platforms. However, the vastness of the maritime areas and the number of vessels to be monitored make permanent monitoring capability difficult, exposing the need for greater sensor capabilities.

Civilian sensors offer a potential complement, especially in the acoustic spectrum. Both ships and anchors can be identified based on the noise they produce and transmit through the water. Civilian hydrophones and AUV-towed sonars can collect data in specific portions of the infrastructure and under certain circumstances (Pilir, 2023; Eleftherakis & Vicen Bueno, 2020). Permanent monitoring could be ensured by the emerging fibre optic sensing technology, in particular, distributed acoustic sensing (DAS).[8] DAS can detect surface vessels and anchors dragged along the seabed within two to three kilometres, providing up to 14 minutes advance warning when trawlers or anchors are approaching the infrastructure (ASN, 2025a). This technology is particularly easy to apply to communications cables, but with more long-term solutions, it can also be used for energy pipelines by adding optical fiber to the infrastructure (Benabid et al., 2025). Furthermore, in addition to the acoustic spectrum, other oceanographic data, such as pressure or magnometric data collected by SMART Cables or AUVs, can help identify anomalies near infrastructure and therefore alert operators or authorities (Eleftherakis & Vicen Bueno, 2020).

[8] This technology transforms existing fibre optic cables into listening devices without adding any external sensors to the infrastructure. It works by connecting specialised measurement equipment to the dry-end of a fibre (e.g. on shore), detecting nanometre-level movements in the fibres and converting these movements into strain measurements similar to acoustic pressure. In particular, laser light pulses are passed down the fibre and some of this light is reflected and scattered by imperfections that are naturally present on each fibre – a process known as “Rayleigh scattering”. Since these imperfections undergo tiny changes in position due to any changes in pressure and the surrounding environment, it is possible to precisely identify the location and source of interference on the cable. (Waagaard, 2022, Bouffaut, 2025),

Attribution

The main difficulty in previous anchor-dragging cases has been attributing the incident. Despite highly suspicious behavior by the crew, it is not easy to attribute the sabotage to the will of a specific state (Staalesen, 2023; Bockmann, 2024; Kärmas 2024). The oceanographic sensors described above could help in the technical attribution. Specifically, academic research has shown that DAS detection can identify vessels based on their engine signatures by triangulating data with AIS and satellite imagery (Thriet et al., 2025). This allows for filling in any gaps that may exist in satellite coverage or in areas where AIS is turned off. In addition, both DAS detection and pressure data can be used to determine the speed, course, and position of the ship (Landrø et al, 2022; Paap et al., 2025; Ratsep et al., 2021). This information can be useful to reconstruct the modalities of the damage and possibly also ascertain the intentionality. It allows to understand whether the vessel veered to hit the infrastructure or adjusted its speed to increase the likelihood of the anchor penetrating the seabed.[9] Conversely, the impact of this data on legal attribution is limited. While constituting unclassified information that can be used as public evidence, intelligence from oceanographic sensors is still unable to establish an effective connection with the will of a state.

Integration

Since intelligence gathering on commercial vessels is generally conducted using public or commercial data, such as AIS or satellite imagery, intelligence sharing with allies should generally not be particularly problematic. One obstacle could arise if data comes from military sensors, such as radar, hydrophones, or sonar. Sharing intelligence from these sensors could compromise the source, revealing information regarding its location or technical characteristics. In this case, information

[9] This data can be very useful in reconstructing the intentionality of the act. In particular, the vessel's cruising speed is an important indicator because the faster the anchor impacts the infrastructure, the greater the damage. Accelerating the vessel's speed shortly before impact would be an indication of an intention to increase the likelihood of damage (Zhang et al., 2022; Bruschi et al., 2018).

sharing could be more difficult, and data from civilian sensors would be a much less demanding alternative. These would allow not to compromise the security of sensitive sources, which is considered by the literature to be one of the main barriers to information sharing (Maras, 2017).

Interference by underwater means

Another attack vector recognized in the literature involves the use of divers, submarines, or uncrewed underwater vessels (UUVs) to damage infrastructure or intercept data flowing through it (Bueger et al., 2022). An example of the use of divers comes from the sabotage of Nord Stream 2, which was allegedly perpetrated using an explosive charge planted by divers (Pancevski, 2024). Evidence of the proven use of submarines to interfere with underwater infrastructure dates back to the Cold War, when, in an operation codenamed Ivy Bells, U.S. Navy submarines tapped a Soviet seafloor communications cable (Polmar, 1996). Finally, evidence of infrastructure interference by UUVs has not yet been documented, but this could occur either with kamikaze drones used as torpedoes to target infrastructure or through more sophisticated UUVs capable of placing explosive charges (Rossiter, 2025).

Detection and Warning

All the acoustic detection methods explained in the previous case study can be used to identify these three submerged attack vectors.[10] However, especially in the case of submarines and UUVs, detection would only occur at closer range, requiring the ability to intervene promptly with naval

[10] For information about detection of divers see: Lo, K. W.; Ferguson, B. G. (2012), "Diver Detection and Localization using Passive Sonar", *Proceedings of the Acoustics*, Fremantle, Australia, https://www.acoustics.asn.au/conference_proceedings/AAS2012/papers/p28.pdf; Zhang, Z. Y. (2007), *Diver Detection Sonars and Target Strength Review and Discussions*, Proceedings of the ICSV14, 14th International Congress on Sound & Vibration, Cairns, Australia, https://www.acoustics.asn.au/conference_proceedings/ICSV14/papers/p221.pdf; Drapp, B. et al. (2025), *Enhancing Coastal Critical Infrastructure Protection with Distributed Acoustic Sensing (DAS)*, UDT 2025 Technical Paper, https://www.apsensing.com/media/1813/download/2025-03%20Enhancing%20Coastal%20Critical%20Infrastructure%20Protection%20with%20Distributed%20Acoustic%20Sensing%20-%20Drapp%20B._DAS_Critical_Infrastructure_Subsea_Cables.pdf?v=1; For information about submarine and UUVs detection see: Strachan, D. R. (2023), "Hearing the Light: DAS could Revolutionize Subsea Defense", *Marine Technology*, https://www.marinetechnologynews.com/news/hearing-light-could-revolutionize-625530

assets available nearby (Strachan, 2023). In addition to acoustic detection, submarines and UUVs can also be detected using data by pressure and acceleration sensors included in the SMART cables Polmar & Whitman, 2017; Navy Lookout, 2021). Although these non-acoustic methods are highly dependent on the specific oceanographic characteristics of the marine areas, such as density and currents, they can constitute a complement to the usual acoustic detection means, especially due to improvements in processing power and oceanographic modeling, which allow for a quicker and more effective analysis of the collected data (Pilir, 2023).

Attribution

Data collected by civilian oceanographic sensors can also play an important role in attribution, albeit with some limitations. Each submarine has its own acoustic signature, a sort of sonic fingerprint resulting from the combination of engine and revolving propeller noise. Naval intelligence agencies have access to a library of signatures from various submarines, both allies and adversaries. By comparing the signals collected by the sensors with the available signatures, they can trace the classification, identification, activity, and capabilities of the vessels (Clark, 2013). Data collected by civilian sensors, once compared with the signatures available to intelligence services, could be useful for attributing sabotage or tapping to a specific state. However, unlike the previous case study, where identification of civilian vessels could be achieved by triangulating the data with AIS and commercial satellite imagery, the need to use the signatures provided by military intelligence to identify underwater platforms constitutes a limitation. This is classified information that could hardly be used as public evidence for political and legal attribution. Two reasons could contribute to this difficulty: first, states may want to keep secret the intelligence efforts that led to the collection of those signatures; second, even if states have plausible factual bases for attributing an attack, they may not want to disclose such evidence, since attackers could learn from those mistakes and avoid leaving the same fingerprints in the future (Tran, 2018). Despite these obstacles, combining naval

intelligence with data from civilian sensors can still be very useful for technical attribution and to support decision-making in case of countermeasures.

Integration

Typically, methods for detecting submerged attack vectors come from military sensors. As in the previous case study, replacing data collected by military technologies with sharing intelligence gathered from civilian sensors could facilitate information exchange, allowing the military source to be preserved.

Cyber Threats

The final case study concerns the potential for cyberattacks against CUI. The increasing digitalization of these infrastructures indeed makes them increasingly exposed to cyber threats (Bueger et al., 2022). Sensors and computers continuously monitor energy pipelines to maintain the flow rate and pressure of the oil or gas and to detect leakages. A sensor spoofing attack can render the sensor useless, thereby keeping the entire system unaware of the leakage (Ammar & Khan, 2024). Attacks can also affect the PLC-based PID controllers, which are used to control flow rate through SCADA software, causing erratic pressure and flows in the pipeline and leading it to leak or explode.[11] In the case of undersea cables, owners or consortia of companies that manage infrastructures use a network management system that allows operators to monitor data traffic, identify cable faults, and add or remove data-transmitting wavelengths (Sechrist, 2012). These systems are vulnerable to a wide range of attacks because they use common operating systems, such as Linux and Windows, and are often connected to remote operations centers via network connections. If a cyberattack were to penetrate one of these systems, hackers would gain control of multiple cable networks and

[11] In 2008, a section of the Baku-Tbilisi-Ceyhan (BTC) pipeline exploded due to a cyber-attack. The hacker got access to the pipeline monitoring system, shut down the alarm warning system and super-pressurized the pipeline, causing it to explode.

data flows, discovering physical vulnerabilities in the cables and gaining the ability to interrupt and divert Internet traffic (*Ibid.*). Although there are no reports of cyberattacks on CUI to date, the vulnerabilities exposed above and examples of similar attacks on terrestrial infrastructure nevertheless allow for an analysis of how oceanographic data could be useful for protection against such threats.

Detection and Warning

Obviously, the primary detection of cyberattacks generally comes from the digital domain. However, underwater oceanographic sensors can help detect cyberattacks that create physical effects in the surrounding environment. In this sense, sensing methods such as DAS can be useful especially in the case of cyber threats to pipelines. In the event of a spoofing attack on pipeline monitoring systems, oceanographic sensors could help identify anomalies not reported by the targeted sensors. Technical literature highlights that DAS can help identify early leaks in the pipeline or changes in oil or gas flow (ASN, 2025b; Ghazali et al., 2024). In synthesis, when infrastructure SCADA monitoring systems are affected by a cyberattack, oceanographic sensors can take over and alert operators before any alterations in flow can seriously damage the infrastructure.

Attribution

Regarding attribution, in this case study, civilian oceanographic sensors cannot help identify the attacker, but they can assist in technical attribution and in tracing the methods used to perpetrate the attack. First, in the initial phase, they can be used to rule out the possibility of a physical interference. Second, they can complement digital detections in understanding the physical effects the cyberattack has had on the infrastructure. Such unclassified information could also be used to provide further evidence for political and legal attribution.

Integration

The information gleaned from oceanographic sensors, while playing a marginal role, can be integrated into intelligence shared with other actors to provide a comprehensive picture of the physical impact of a cyberattack. This information could be useful in preventing similar attacks by observing how the infrastructure reacted to certain flow manipulations or what physical alterations the attacker exploited to damage the infrastructure. Such unclassified and non-sensitive information can be easily exchanged because it does not contain private client data or information that a hostile entity could exploit in the event of an information leak.[12]

Conclusions

The article analyzed the role of civilian oceanographic sensors in intelligence collection to protect CUI. The initial hypothesis, according to which civilian sensors can contribute, with some limitations, to improving detection, attribution, and intelligence sharing, is confirmed by the empirical analysis. This examined the potential role of civilian sensors in three possible scenarios of infrastructure attacks (weaponization of civilian vessels, interference by submerged attack vectors, and cyberattacks).

Civilian oceanographic sensors demonstrate the greatest potential in threat detection and warning. Comparison of the technical capabilities of these sensing methods with the various possible attack vectors reveals the ability to identify different types of threats and provide a warning to authorities.

From the perspective of intelligence sharing, the ability to replace classified information with unclassified but equally useful intelligence is a significant advantage, as it allows the preservation of sensitive sources, the security of which is generally one of the main barriers to information sharing.

Data collected by civilian sensors also present potential benefits concerning attribution, albeit with greater limitations. They have proven particularly useful for technical attribution, allowing the

[12] Privacy concerns and the possibility of a Man-in-the-Middle attack that intercepts information during exchange and then exploits it for a subsequent cyberattack are two of the main barriers to cyber-intelligence sharing (Wagner, 2019).

identification of attack vectors through signature comparison and the reconstruction of the methods used. Conversely, they have a more limited impact in the case of political and, above all, legal attribution. Data from civilian sensors, although in some cases able to help identify a vessel or submarine, are not sufficient to satisfy the legal requirements for attribution, because they either fail to establish effective state control over the vessel or require comparison with naval intelligence signatures that cannot be used as public evidence.

The analysis provides an initial contribution to analyzing the potential role and limitations of civilian sensors in protecting CUI, but this presents several limitations and gaps that should be explored further by academia across various fields and disciplines. Regarding warning capabilities, this article has not explored in detail how the potential detection ranges and response times that civilian sensors could provide for authorities might be affected by different environmental conditions (e.g., water depth, noise level generated by commercial traffic, etc.) or different submerged attack vectors (submarines, UUVs or divers). In this sense, greater input from the technical literature is needed for technologies that are still essentially new. Regarding attribution, further studies are needed on the legal mechanisms that allow the use of classified information in court in various European states, such as *ex parte* or *in camera* provisions. Finally, from the perspective of intelligence sharing, it is necessary to conduct a more in-depth study on the mechanisms that regulate the circulation of data collected by private sensors, such as those of companies that own the infrastructure.

Bibliography

Ammar, M. and Khan, I. A. (2024), “Cyber Attacks on Maritime Assets and their Impacts on Health and Safety Aboard: A Holistic View”, *ArXiv*, Cornell University, https://arxiv.org/html/2407.08406v1#bib.bib44

ASN (2025a), *Written evidence submitted by Alcatel Submarine Networks Use of fibre sensing to secure UK subsea infrastructure*, https://committees.parliament.uk/writtenevidence/138747/pdf/

ASN (2025b), “Offshore Oil and Gas DAS Applications”, https://www.asn.com/offshore-oil-and-gas-das-applications/;

Benabid, M.-K., Baumgartner, P., Jin, Ge and Fan, Y. (2025), “Leakage Detection Using Distributed Acoustic Sensing in Gas Pipelines”, *Sensors*, *25*(16), 4937, https://doi.org/10.3390/s25164937

Besch, S. & Brown, E. (2024), *Securing Europe’s Subsea Data Cables*, Carnegie Endowment for International Peace, Washington DC, https://carnegie-production-assets.s3.amazonaws.com/static/files/Besch%20Brown-Europe%20Subsea%20Cables.pdf

Bockmann, M. W. (2024), “Russia-linked cable-cutting tanker seized by Finland ‘was loaded with spying equipment’, *Lloyd’s List*, https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment

Bouffaut, L. (2025), “Distributed Acoustic Sensing (DAS) for Marine Conservation”, *K. Lisa Yang Center for Conservation Bioacoustics*, Cornell University, https://www.birds.cornell.edu/ccb/distributed-acoustic-sensing-das-for-marineconservation/#:~:text=Distributed%20Acoustic%20Sensing%E2%80%94or%20DAS,and%20densely%20sampled%20listening%20arrays.

Bruschi, R., Bartolini, L., Vitali, L. (2018), *Protecting Offshore Pipelines from External Interferences: Dropped and Dragged Anchors*, Abu Dhabi International Petroleum Exhibition & Conference, Abu Dhabi, UAE. Accelerating the vessel's speed shortly before impact would be an indication of an intention to increase the likelihood of damage.

Bueger, C. and Liebetrau, T. (2023), “Critical maritime infrastructure protection: What’s the trouble?”, *Marine Policy*, 155, 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*, European Parliament

Byman, D. (2025), “Improving US Intelligence Sharing With Allies and Partners”, *Center for International and Strategic Studies*, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-01/250128_Byman_Intelligence_Sharing.pdf?VersionId=dTE404K_zq877C6RONG14Y5b_Ge3JHBf

Cannon, B. J. and Bhaat, P. (2024), *Policy Recommendations for Quad Cooperation On Submarine Cable Protection in the Indopacific*, PacNet, Pacific Forum, Honolulu, HI

Clare, M. (2022), *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), Issue 4

Clare, M. (2022), *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), Issue 5

Clare, M. (2024), *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), Issue 8

Clark, B. (2015), *The Emerging Era in Undersea Warfare*, Center for Strategic and Budgetary Assessments (CSBA)

Clark, R. M. (2013), *Intelligence Collection*, SAGE Publications, CQ Press, Thousand Oaks, CA

Corbett, S. and Danoy J. (2022), "Beyond NOFORN: Solutions for increased intelligence sharing among allies", *Atlantic Council*, Issue Briefs, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence-sharing-among-allies/

Coté Jr., O. (2012), "Assessing the Undersea Balance Between the U.S. and China", in T. G. Mahnken (ed), *Developing Competitive Strategies for the 21st Century: Theory, History and Practice*, Stanford University Press, Palo Alto: CA

Council of the European Union (2022), *Implementing Guidelines For The Framework For A Coordinated EU Response To Hybrid Campaigns*, https://data.consilium.europa.eu/doc/document/ST-15880-2022-INIT/en/pdf;

Davenport, T. (2023), *Intentional Damage to Submarine Cable Systems by States*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2305, https://www.lawfaremedia.org/article/inten tional -damage-to-submarine-cable-systems-by-states

Eleftherakis, D. & Vicen-Bueno, R. (2020), "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors"

European Commission (2024), *Outsmart Malicious Actors To Deter Hybrid Attacks*, https://commission.europa.eu/document/download/934d5577-2d06-4cef-8aa3-8edd2556dd59_en?filename=2024_Niniisto-factsheet_6.pdf

European Commission (2025), *EU Action Plan on Cable Security*, https://ec.europa.eu/newsroom/dae/redirection/document/113049

Fearon, J. D. (1991), "Counterfactuals and Hypothesis Testing in Political Science", *World Politics*, 43(2), pp. 169-195

Ghazali, M. F., Mohamad, H., Yusoff, M., Nasir, M., Hamzh, A., Abdullah, M. A., Faiqa, N. and Aziz, A., Thansirichaisree P., Saiful, M. and Zan, D. (2024), "State-of-the-Art application and challenges of optical fibre distributed acoustic sensing in civil engineering", *Optical Fiber Technology*, 87, https://www.sciencedirect.com/science/article/pii/S1068520024002566#s0010

Giannopoulos, G., Smith, H., Theocharidou, M. eds. (2021), *The Landscape of Hybrid Threats: A Conceptual Model Public Version*, Hybrid CoE

Gilli, A., Gilli, M., Ricchi, A., Russo, A. and Carniel, S. (2024), "Climate Change and Military Power: Hunting for Submarines in the Warming Ocean", *Texas National Security Review*, 7(2), pp. 16-41,

Hanna, M., Granzow, D., Bolte, B. and Alvarado A. (2017), "NATO Intelligence and Information Sharing: Improving NATO Strategy for Stabilization and Reconstruction Operations", *Connections QJ*, 16 (4), pp. 5-33, https://doi.org/10.11610/Connections.16.4.

Hendriks, M. S. and Halem, H. (2024), *From Space to Seabed Protecting The UK's Undersea Cables from Hostile Actors*, Policy Exchange, Westminster, London

Hioe, B. (2025), “Another Severed Submarine Cable Raises Alarm in Taiwan”, *The Diplomat*, https://thediplomat.com/2025/01/another-severed-submarine-cable-raises-alarm-in-taiwan/

Humpert, M. (2022), “Fiber-optic Submarine Cable near Faroe and Shetland Islands Damaged; Mediterranean Cables also Cut”, *High North News*, https://www.highnorthnews.com/en/fiber-optic-submarine-cable-near-faroe-and-shetland-islands-damaged-mediterranean-cables-also-cut

Hybrid CoE (n.d), “Defintion of Hybrid Threats”, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Kärmas, M. (2024), “Balticconnector case more sabotage than an accident, experts say”, *ERR News*, https://news.err.ee/1609255413/balticconnector-case-more-sabotage-than-an-accident-experts-say

Landrø, M., Bouffaut, L., Kriesell, H. J., Potter, J. R., Rørstadbotnen, R. A., Taweesintananon, K., Johansen, S. E., Brenne, J. K. Haukanes, A., Schjelderup, O. & Storvik, F. (2022), “Sensing whales, storms, ships and earthquakes using an Arctic fibre optic cable”, *Sci Rep*, 12, https://doi.org/10.1038/s41598-022-23606-x

Lasoen K. (2022), *Realising the EU Hybrid Toolbox: Opportunities and Pitfalls*, Clingendael Netherlands Institute of International Relations, https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf;

Leicester, J. & Burrows, E. (2025), “At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard”, *AP News*, https://apnews.com/article/nato-france-russia-baltic-cables-ships-damage-764964a275530915c2cc5af1125ec125

Maras, M.-H. (2017) “Overcoming the intelligence-sharing paradox: Improving information sharing through change in organizational culture”, *Comparative Strategy*, 36(3), pp. 187-197, DOI:

Morris, J. L. & Clark, R. M. (2015), “Measurement and Signal Intelligence” in Lowenthal, M. M. & Clark, R.M. eds., *The Five Disciplines of Intelligence Collection*, CQ Press

Morris, J. L. (1996), “MASINT,” *American Intelligence Journal*, 17 (1/2), p. 24

National MASINT Office (2022), *MASINT: A Surface Level Look Into a Misunderstood Intelligence Discipline*, Defense Intelligence Agency (DIA), https://www.dni.gov/files/ODNI/documents/21-113_MASINT_Primer__2022.pdf

NATO (2023), “NATO stands up undersea infrastructure coordination cell”, https://www.nato.int/cps/en/natohq/news_211919.html

Navy Lookout (2021), “Royal Navy submarines and non-acoustic sensor technology”, https://www.navylookout.com/royal-navy-submarines-and-non-acoustic-sensor-technology/

Ned Lebow, R. (2015), “Counterfactuals and Security Studies”, *Security Studies*, 24(3), pp. 403-412, DOI: 10.1080/09636412.2015.1070605

Nilsson, N., Weissmann, M., & Palmertz, B. (2025), “Hybrid Threats and the Intelligence Community: Priming for a Volatile Age”, *International Journal of Intelligence and CounterIntelligence*, pp. 1–23. https://doi.org/10.1080/08850607.2024.2435265

Paap, B., Vandeweijer, V., van Wees, J.-D. and Kraaijpoel, D. (2025), “Leveraging Distributed Acoustic Sensing for monitoring vessels using submarine fiber-optic cables”, *Applied Ocean Research*, 154 (104422), https://doi.org/10.1016/j.apor.2025.104422;

Pachaiyappan, P., et al. (2024), “Enhancing Underwater Object Detection and Classification Using Advanced Imaging Techniques: A Novel Approach with Diffusion Models”, *Sustainability*, *16*(17), 7488. https://doi.org/10.3390/su16177488

Pancevski, B. (2024), “A Drunken Evening, a Rented Yacht: The Real Story of the Nord Stream Pipeline Sabotage”, *The Wall Street Journal*, https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c

Pancevski, B. (2024), “Europe Sees Signs of Russian Sabotage but Hesitates to Blame Kremlin”, *The Wall Street Journal*, https://www.wsj.com/world/europe/europe-sees-signs-of-russian-sabotage-but-hesitates-to-blame-kremlin-72598d4b?mod=article_inline

Pilir, R. (2023), “Scientists: Estonia could monitor undersea infrastructure with microphones”, *ERR*, https://news.err.ee/1609135955/scientists-estonia-could-monitor-undersea-infrastructure-with-microphones; Eleftherakis, D. & Vicen-Bueno, R. (2020), “Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors”, *Sensors*, 20

Pilir, R. (2023), “Scientists: Estonia could monitor undersea infrastructure with microphones”; Clark, B. (2015), *The Emerging Era in Undersea Warfare*, p. 15

Polmar, N. (1996), “The U.S. Navy: How Many Spy Subs . . .?”, *Proceedings*, 122 (12), pp. 1-126

Polmar, N. and Whitman, C. (2017), “Russia Poses a NonAcoustic Threat to U.S. Subs”, *Proceedings*, 143 (10), pp. 1-376

Ratsep, M., Parnell, K. E., Soomere, T., Kruusmaa, M. (2021), “Surface vessel localization from wake measurements using an array of pressure sensors in the littoral zone”, *Ocean Engineering*, 233, https://doi.org/10.1016/j.oceaneng.2021.109156

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

Sechrist, M. (2012), *New Threats, Old Technology: Vulnerabilities In Undersea Communications Cable Network Management Systems*, Belfer Center for Science and International Affairs, Harvard Kennedy School

Siman, B. (2023), “Hybrid Warfare: Attribution is Key to Deterrence”, *Egmont Royal Institute for International Relations*, https://www.egmontinstitute.be/hybrid-warfare-attribution-is-key-to-deterrence/

Singh, A. (2023), “The Promise and Pitfalls of Underwater Domain Awareness”, *War On the Rocks*, https://warontherocks.com/2023/02/the-promise-and-pitfalls-of-underwater-domain-awareness/;

Sislin, J. D. (2019), “Underappreciated, Underrepresented: Thoughts on Teaching MASINT. American Intelligence Journal”, 36(2), pp. 28–39. https://www.jstor.org/stable/27066370

Staalesen, A. (2023), “Runaway ship Newnew Polar Bear, suspected of sabotage in Baltic Sea, is sailing into Russian Arctic waters”, *The Barents Observer*, https://www.thebarentsobserver.com/security/runaway-ship-newnew-polar-bear-suspected-of-sabotage-in baltic-sea-is-sailing-into-russian-arctic-waters/164423

Stone, C. M., *Deterrence in Space: Requirements for Credibility*, National Institute for Public Policy, Information Series, No. 471, https://nipp.org/wp-content/uploads/2021/03/IS-471.pdf

Strachan, D. R. (2023), “Hearing the Light: DAS could Revolutionize Subsea Defense”, *Marine Technology*, https://www.marinetechnologynews.com/news/hearing-light-could-revolutionize-625530

Taddiken, B. & Krock, K. (2021), “66 Years of Undersea Surveillance”, *Naval History*, 35 (1), https://www.usni.org/magazines/naval-history-magazine/2021/february/66-years-undersea-surveillance.

Thiriet, P., Lecoulant, J., Labat, V., Boudraa, A.O. and Astolfi J.-A. (2025), "Distributed Acoustic Sensing for Ship Detection and Identification," *OCEANS 2025 Brest*, Brest, France, doi: 10.1109/OCEANS58557.2025.11104529

Tran, D. (2018), “The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack”, *The Yale Journal of Law & Technology,* 20

Tyack, P. L. et al. (2021), “Measuring ambient ocean sound during the COVID-19 pandemic”, *Eos,* 102, https://doi.org/10.1029/2021EO155447

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

Waagaard O H. (2022), “Listening across the oceans: Distributed acoustic sensing”, *Research Outreach*, 131, https://researchoutreach.org/articles/listening-across-the-oceans-distributed-acoustic-sensing/

Wagner, T. D. (2019), “Cyber threat intelligence sharing: Survey and research directions”, *Computers & Security*, 87, https://www.sciencedirect.com/science/article/pii/S016740481830467X

Waite, A. D. (2001), *Sonar for Practising Engineers – 3rd ed*., Wiley, Chilchester, UK

Wall, C. and Morcos, P. (2022), “Invisible and Vital: Undersea Cables and Transatlantic Security”, *Center for Strategic and International Studies*, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Wolfberg, A. (2024), *Climate Security Intelligence: From Knowledge Transfer to Co-Creation*, Springer Nature Switzerland

Zhang T., Du, A., Li, L., Wei, R., Tan, H. and Wang, K. (2022), "Analysis of Three-Core Composite Submarine Cable Damage Due to Ship Anchor," *IEEE Access*, 10, pp. 93910-93920, 2022, doi: 10.1109/ACCESS.2022.3203589;