Journal on Baltic Security, 2026; 12(1): 1- 27

Research Article

Open Access
https://doi.org/10.57767/jobs_2026_003

Hans Liwång*, Thomas Frisk, Jonas Kindgren, Johan Sigholm, Nicolò Boschetti, Oskar Frånberg, and Gregory Falco**

Situational Awareness for Proactive Rerouting: Enhancing Resilience in Submarine Communication Cables

Received : 08 August 2025.
Accepted : 28 October 2025.

Abstract: Suspected sabotage to submarine communication cables (SCCs) across the world has raised questions about the resilience of these systems. Data communication networks typically use a network approach, which spreads the networks' capacity across diverse routes to provide redundancy. This study takes a risk mitigation and resilience perspective by investigating the information needed to support proactive rerouting decision-making. This study reveals that appropriate situational awareness is dependent on specific, real-time information about hazards and threats to the cable in question. For an operator of an SCC, such a contribution is not possible without being interpreted as an integral stakeholder in defence.

* **Corresponding author: Hans Liwång**, email: hans.liwang@fhs.se, Department of Systems Science for Defence and Security, Swedish Defence University, Stockholm, Sweden and Department of Engineering Mechanics, KTH Royal Institute of Technology, Stockholm, Sweden.
** **Authors: Thomas Frisk**, Department of Systems Science for Defence and Security, Swedish Defence University, Stockholm, Sweden. **Jonas Kindgren**, Department of Systems Science for Defence and Security, Swedish Defence University, Stockholm, Sweden and Department of Mathematics and Natural Sciences, Blekinge Institute of Technology, Karlskrona, Sweden. **Johan Sigholm**, Department of Systems Science for Defence and Security, Swedish Defence University, Stockholm, Sweden. **Nicolò Boschetti**, Sibley School of Mechanical and Aerospace Engineering, Cornell University, Ithaca, NY, USA. **Oskar Frånberg**, Department of Mathematics and Natural Sciences, Blekinge Institute of Technology, Karlskrona, Sweden. **Gregory Falco**, Sibley School of Mechanical and Aerospace Engineering, Cornell University, Ithaca, NY, USA.

Keywords: Submarine Data Communication; Situational Awareness; Hazards and Threats; Cybersecurity; Systems Science for Defence and Security; Distributed Acoustic Sensing; Decision-Making.

Introduction

The defence challenges at sea have changed because of new technology (Wills, 2020); this change includes an increase in the number of submarine communication cables (SCCs). Recent events in the Baltic Sea and around Taiwan where damage, and suspected sabotage, raised questions about the resilience of these systems (Milmo, 2025). A single modern SCC can carry data upwards of a petabit per second and these cables carry almost all intercontinental internet traffic. There are also many other cables for power transmission and traditional telephony. These cables – often lying openly on the seabed of our oceans – not only are potentially susceptible to damage but also manipulation of the optical fibres used to transmit data or cyberattacks targeting the network infrastructure, which could compromise the integrity and confidentiality of communications relying on the SCCs (Boschetti and Falco, 2025).

Data communication networks typically use a network approach, which spreads the network's capacity over multiple routes to provide redundancy (Jain et al., 2022; US GAO, 2022). In the event of a single SCC failure, the network traffic is rerouted over other cables while the service is restored to the damaged infrastructure (Gordon and Jones, 2022). Therefore, single failures of SCCs have low or very limited consequences for data communications. While straightforward, this approach is not always sufficient for critical communications, which cannot afford new security risks induced by insecure routes or (rare but possible) disconnections. Moreover, modern mesh networks are susceptible to cascading failures because of disruptive malware propagation. A large part of society can be affected in scenarios where critical infrastructure and critical communications rely on a single SCC or if mainstream management software is compromised (Boschetti and Falco, 2025).

Managing submarine cables is an inherently multiagency, regulatory, and often international issue (Bueger and Liebetrau, 2021), where several different state and commercial value perspectives overlap (Wetter and Wüthrich, 2015). This multiagency, regulatory, and international issue presents a challenge to operations, and the response is being studied in parallel domains (Boschetti et al., 2025; Sigholm, 2016; US GAO, 2022). Organisations such as the International Cable Protection Committee (ICPC) and the International Telecommunication Union (ITU) offer guidelines and recommended practices for cable protection. However, there are possible practical gaps in coordinated threat response if practice is not adapted to the complex combination of threats, hazards and actors of today.

The important functions of society must be resilient (Roepke and Thankey, 2019). Therefore, irrespective of whether there is an antagonistic attack behind the disturbance to an SCC or not, there is a need to mitigate the effects of disturbances by introducing new data communication alternatives and a balanced and proactive logic for rerouting data. No single actor can provide the information needed for situational awareness in such decision-making. The information needed is potentially spread over both military and civilian actors as well as over both public and private actors. Therefore, to support the development of a more balanced and proactive logic for rerouting data, this study investigates the possible information contributions that can be provided by different stakeholders of the maritime domain.

The main rerouting alternative considered in this study is an extended and controlled rerouting of data through space or other alternatives that are independent of seabed hazards and threats. However, such an alternative possibly comes with other costs, risks, and threats, including a likely reduction in transmission capacity. Although recent advances in free-space optical communication have allowed for data links between Earth and satellites in orbit, as well as between satellites themselves, the overall capacity of submarine cables cannot be matched by satellite-based solutions (Boschetti and Falco, 2025). The threat of jamming, eavesdropping, cyberattacks, and physical sabotage of space communications systems is also a factor that must be considered. A balanced combination of conceptually different

solutions, such as SCCs and space-based solutions, may highlight the strengths and mitigate weaknesses of specific solutions.

The focus of this study is on a specific SCC (here denoted SCC0) the operator of SCC0 – typically a commercial and civilian organisation. This study considers the information the operator could utilise about hazards, threats and disturbances to SCC0 and about the consequences of rerouting the data. From this perspective, challenges such as the availability of suitable information and the ability to share information between commercial and public organisations and between civilian and military organisations exist.

This study is performed from an applied utilitarian perspective, i.e., it aims both to identify current stakeholder possibilities and to propose concepts for creating capability for suitable situational awareness for decision support, where value is defined by contributions to risk mitigation and resilience. Risk mitigation and resilience are further defined in a following section 'Foundational Concepts: Risk Mitigation, Resilience, and Situational Awareness' below. This study is normative and conceptual and uses various literature sources and theoretical approaches. It analyses the proposed development from a sociotechnical perspective and in terms of interlinked relevance and rigor assessments.

Theoretical Framework and Research Approach

To support the qualitative assessments and develop concepts for resilient situational awareness this study combines theoretical concepts for capability development, risk mitigation, and resilience. This section first describes these theoretical concepts and then how they are combined in the research approach.

A Capability Perspective

Support for the development of solutions that bridge civilian and military sectors and interests is lacking (Adlakha-Hutcheon et al., 2018; Liwång, 2022; NATO STO, 2021). There is also limited support for developing system designs that combine and span findings from areas such as engineering, management, and social sciences into a consistent approach (Winter, 2008). Therefore, a 'capability' perspective is used here to put focus on top-level system design and how a set of organisations

arranges resources to meet common goals (Grabis, Zdravkovic, and Stirna, 2018; Liwång et al., 2023; Yue and Henshaw, 2009).

The capability concept determines aspects such as what type of technology is needed, how it is expected to interact with personnel, and what competence is needed. This refers to creating a conceptual design that connects development at several different societal levels and types of actors, i.e., an important but challenging link between policy and technology development (Liwång, 2022). With the capability perspective the assessment in this study focuses on solutions for situational awareness with extensive interactions between social and technical components, where important system characteristics and capabilities are emergent properties of the system.

Risk Mitigation, Resilience, and Situational Awareness

In this study, we define risk mitigation as the means to reduce any or all the following risk components: likelihood, consequence, and uncertainty (see Aven, 2009; Bakx and Nyce, 2015; Liwång, 2017; Liwång, Ericson, and Bang, 2014; NATO NSO, 2024). Resilience, as defined here, is the ability to protect the core goals of a system against changes and events outside the system. It is detailed here in terms of the five processes of anticipation, monitoring, response, recovery, and learning according to Lundberg and Johansson (2015):

- Anticipation represents being able to consider, before the fact, that a situation might occur and to act based on this prediction.
- Monitoring represents the ability to detect, make sense of, and act based on the discovery of an event's onset.
- Response represents the ability to act during an unfolding event.
- Recovery represents the ability to address restoration after disruptions, ideally rebuilding with improved capabilities and reduced vulnerability.
- Learning represents the ability to adjust the system in the aftermath of an event, learning from both positive and negative outcomes.

The reliability of a system has strong connections to risk mitigation and resilience and is referred to here as a function of redundancy and diversity. Redundancy is a physical feature of the infrastructure that provides alternative routes through the system, and diversity is the insensitivity to common-cause failures within the system (Andrews and Moss, 2002; Möller and Hansson, 2008). The work with risk mitigation and resilience must be active and integrated into management, planning, and decision-making, where risk is accepted if benefits outweigh potential losses (Liwång, Ericson, and Bang, 2014; NATO NSO, 2024).

Risk mitigation and resilience are dependent concepts; risk mitigation is an integral part of resilience (Lundberg and Johansson, 2015). Therefore, the two concepts are combined here to define the following three situational awareness information-gathering capabilities (SA1–SA3), developed from the concepts of risk mitigation and resilience described above:

- SA1: Information for anticipation: Information from incidents and near misses that can be translated into risk models related to possible future hazards and threats.
- SA2: Monitoring to provide information for response to reduce likelihood and consequence: Information about activities and events related to SCC0 that indicate its status and any hazards or threats, enabling proactive or reactive measures to reduce likelihood or consequences and to support recovery.
- SA3: Monitoring to provide information for learning and for reducing uncertainties: Information about activities and events that make it possible to explain occurrences and attribute antagonistic actions.

Suitable situational awareness is understood here as a capability that provides for SA1–SA3, where SA2 ideally supports both proactive response and reactive response and recovery.

Research Approach

To generate new knowledge about the problem domain both rigour and relevance must be assured throughout the process (Dansarie, Andersson, and Silfverskiöld, 2025). Therefore, inspired by Hevner (2007), this study includes relevance through

initiating the process by defining the application domain. To ensure rigor there must also be a thoroughly referenced knowledge base of scientific foundations, i.e., the selection and application of appropriate theories and methods for constructing and evaluating the proposed solution (Hevner et al., 2004; Hevner, 2007). The qualitative assessment provided by such a combination of relevance and rigor is suitable for developing an understanding of complex sociotechnical systems (Mauri and Antonovsky, 2021).

To ensure both relevance and rigor this study is divided into three steps. The first step describes the characteristics of the possible stakeholder situational awareness contributions, presented as layers of possible information. This first step represents the relevance and the application domain and introduces contextual knowledge into the assessments. The second step qualitatively evaluates the possible situational awareness capability contribution from each layer using the three information-gathering capabilities (SA1-SA3) defined above. Therefore, step two represents rigor ensuring scientific foundations in the evaluation of the different contributions to situational awareness. Steps one and two are both reported in the subsection '*Steps 1 and 2: Information Layers and Their Possible Contributions to Situational Awareness'*.

The subsection *'Step 3: Evaluation of the Situational Awareness Created and the Possibility of Increasing Risk Mitigation and Resilience'* iterates between the relevance and rigor contributions and thereby examines and evaluates the findings from a system perspective, especially in terms of sociotechnical integration and governance aspects.

Results

Steps 1 and 2: Information Layers and Their Possible Contributions to Situational Awareness

This section describes the characteristics of the possible stakeholder contributions, introduces contextual knowledge, and evaluates the possible contribution from each layer using the three information-gathering capabilities (SA1–SA3) as defined above.

Figure 1 shows the layers of society that could provide information about technical status, threats, and risk. Each of these layers contains components in terms of organisations, processes, rules, and technology, and the characteristics of each layer are a product of these system components.

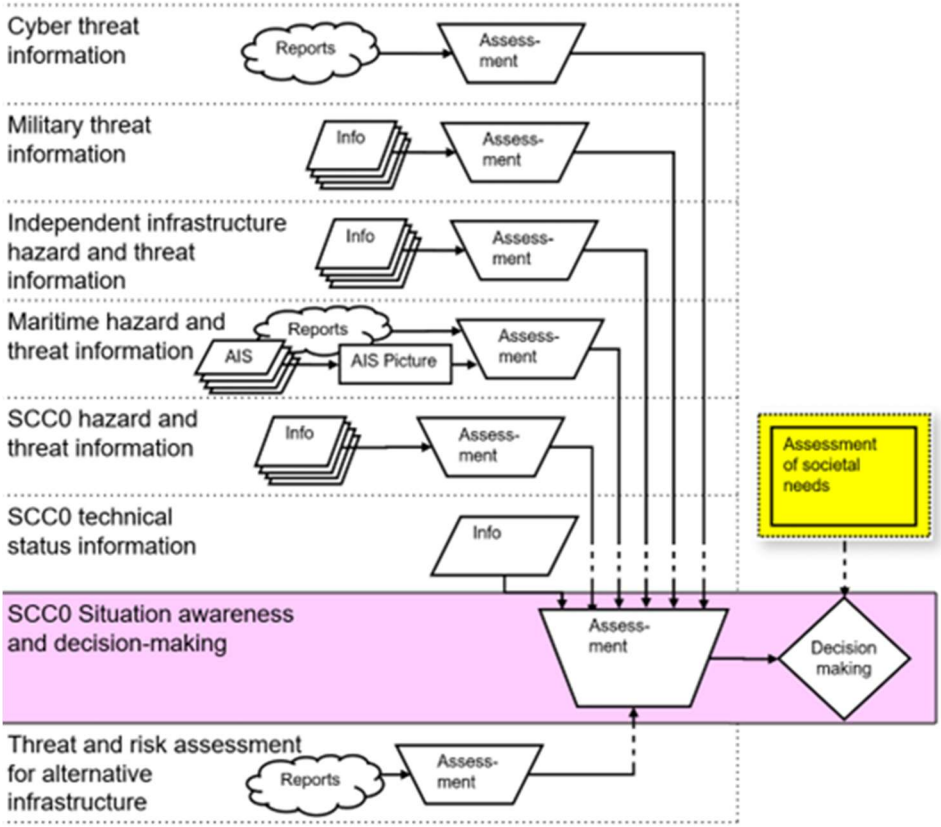

Figure 1. *A flowchart illustrating the conceptual architecture for information about the technical status, hazards, threats, and threat level with which different layers could contribute.*

Below is a description and assessment of the possible contribution to situational awareness from each layer, starting from SCC0 (the SCC in focus) and working outwards. The assessment results are summarised in Table 1.

SCC0 Technical Status Information

This is a fully automated technical layer containing information about the technical status of the SCC0, typically indicating whether the connection is 'operational' or 'down'. Modern digital systems include continuous functions for checking transmission functionality and pinpointing the location of any disturbance.

Precise, immediate information about infrastructure status is central to acting on malfunctions and initiating further investigations. Often, at sea, distant or external resources are needed for both investigation and repair. Therefore, precise status information saves time and resources in coordinating the next steps. Information from the SCC0 technical status layer cannot be replaced by other external information.

SCC0 Hazard and Threat Information

Monitoring and detecting undersea cable hazards and threats is an active field of research. This layer collects and processes sensor data operated by the SCC0 itself. Hazards exist in the physical domain but can also target the information carried by the cable.

In SCC0 monitoring, the optical fibres built into the cable are used as sensors that can monitor infrastructure changes, errors, or nearby activity, including techniques such as fibre optic cables (FOC) distributed temperature sensing (DTS) and FOC distributed acoustic sensing (DAS) (see Duckworth et al., 2013; Gutscher et al., 2019; Gutscher et al., 2023; Howe et al., 2022; OX2, 2025; Taweesintananon et al., 2021; Thodi et al., 2014).

Cables are often partially buried in the seabed for risk mitigation (Olsson, Franberg, and Kulesza, 2022). Therefore, by using DTS and data about the surrounding environment for calculating cable burial depth, operators can identify potential issues early, minimise damage, and reduce the need for frequent physical surveys (Howe et al., 2022; Thodi et al., 2014).

DAS technology transforms an optical fibre into a long, densely sampled acoustic/seismic sensor array. It can detect and classify multiple threats, such as digging and tunnelling, footsteps, and gunshots, with high location accuracy over considerable distances. Previous research and testing have demonstrated successful applications in a variety of environments, with coverages up to 50 km and virtual sensor separations as small as one metre (see Duckworth et al., 2013; Howe et al., 2022; OX2, 2025; Tejedor et al., 2017; Thodi et al., 2014). Such information can enable proactive actions to prevent cable damage.

Interference with the optical cable can also be detected via optical time domain reflectometers (OTDRs), which can identify and characterise the type of tampering that occurs (Bhatta et al., 2019; Tejedor et al., 2017). As activities close to or on the cable are rare, signals detected from these built-in sensing functions (i.e., DTS, DAS and OTDRs) typically warrant prompt mitigation.

The confidentiality and integrity of the data transmitted via SCCs could also be compromised through physical tampering of the optical fibres or seabed amplifiers. Such an attack is technically possible but highly complex and requires a high level of sophistication due to the challenging environmental conditions on the seabed (Boschetti and Falco, 2025). However, such an attack could have severe consequences because it may not trigger any alarms if the cable is without protection.

Continuous data from DTS and DAS on activity on or near a cable also would provide information on both the baseline activity and near misses, information that is not currently registered. This information provides context for more severe incidents and thereby contributes to more developed anticipation and learning.

Maritime Hazard and Threat Information

This layer collects vessel traffic data from sources such as automatic identification system (AIS) transceivers and shore-based radars. Space-based systems can also provide better coverage than can assets on the ground. This information is continuously monitored and assessed through manual and automatic anomaly detection (Relling et al., 2022).

Information about vessel traffic and ship behavioural anomalies is important for understanding the likelihood of hazards such as fishing accidents or anchor dragging. However, most shipping anomalies do not affect seabed cables. Therefore, specific real-time subsea data are needed to identify which surface vessels present hazards or threats to seabed infrastructure.

Independent Infrastructure Hazard and Threat Information (Surveillance and Inspection with Ships or Underwater Vehicles)

One approach is to use dedicated autonomous underwater vehicles to patrol cables and relay footage for analysis. These systems are used for in situ pipeline and cable inspection (Evans et al., 2003; Hamilton and Evans, 2005). However, low underwater operation speeds (approximately 10 knots), short sensor and communication ranges (1–100 m), and limited bandwidths (Tärnholm and Liwång, 2022b) make immediate response challenging. Thus, even with multiple vehicles patrolling every cable, the response time is too long for detecting or mitigating ongoing incidents.

Regular external inspections or surveillance can identify deteriorating environmental conditions or sabotage preparations that are useful for anticipating future incidents. However, such implementation is resource intensive.

Military Threat Information

In this layer, military organisations collect data from sensors and assets, often from vessels (including autonomous ones), and make qualitative threat-level assessments. Routine surveillance of the seabed and underwater infrastructure helps establish a baseline and detect changes over time, reducing uncertainty about threats and antagonistic events. The use of military assets in creating situational awareness results in a variety of capabilities that civilian actors do not possess, as the use of the military is shaped to handle other types of conflict and adversaries. The use of military assets is, however, not uncomplicated in times of peace because of contributing nations' legal frameworks as well as international agreements (Tärnholm and Liwång, 2022a). Potential capabilities could be surface ships with

flying assets with long-range sensors such as radars and signal intelligence but also submarines and the ability to act with enough force to handle a confirmed threat to a SCC. Another important aspect is the possible deterrent effect military assets have on potential threat actors (Till, 2009).

Detailed and high-quality routine surveillance of the seabed and underwater infrastructure is important for establishing a baseline description of activity and detecting changes over time. Such information is important for the development of the ability to foresee and predict future events and to identify previously unexampled events important for anticipating events (Lundberg and Johansson, 2015) and therefore reduces the uncertainty about threats and antagonistic events.

Cyber Threat Information

In this layer, an organisation – often a nonmilitary government agency – collects information about cyber incidents and makes manual qualitative assessments of the cyber threat level. Several SCC management vulnerabilities are related to cyber threats, including supply chain compromise, where the limited market of SCC software providers poses a particular risk. Infiltration at any point – from software creation to update distribution – can compromise entire networks and thus affect wide ranges of users within the government and private sectors (Sherman, 2021; US GAO, 2022). Moreover, weak encryption and poor key management practices can further jeopardise the cybersecurity of SCCs (Furdek et al., 2021). Understanding these threats helps anticipate future incidents, learn from events in other sectors (Lundberg and Johansson, 2015), and therefore reduce uncertainty about the future.

Hazard and Threat Information About Alternative Infrastructure

This layer evaluates threats and risks to terrestrial and space-based infrastructure, which is crucial for rerouting decisions. Information about hazards in space is of particular interest because space-based communications are independent of seabed threats. Ongoing development of low-Earth orbit (LEO) satellite communications technology, increased spectrum use, and optimised antennas with more advanced beamforming and digital processing technologies, will allow LEO constellations to provide significantly higher throughput rates in the coming years (Brodkin, 2024). When also considering the potential to leverage multiple satellites in parallel to

transmit and receive data and recent developments in free-space optical communication – using laser light to transmit data within an optical fibre – satellite communication is gradually becoming a realistic option for providing redundancy for terrestrial communication infrastructures (Potter, 2024).

However, space-based infrastructure has its own systemic vulnerabilities. Examples of naturally occurring phenomena that can hamper communication with or between satellites include adverse weather conditions in the atmosphere (e.g., fog and sandstorms) and space (e.g., solar flares and electromagnetic radiation) (Buzulukova and Tsurutani, 2022). In the future, a proliferated LEO environment or a so-called Kessler syndrome scenario (Kessler et al., 2010) caused by a growth in space debris could have detrimental effects on space operations in certain orbits (Luu and Hastings, 2022). Moreover, several cyber threats exist in relation to space data communications (Falco et al., 2024).

Of particular interest is the knowledge about alternatives that are independent of the weaknesses of SCC0, i.e., alternatives that offer increased diversity in the system. Space-based systems are an example of an alternative that contributes substantial diversity to the system.

Assessment of Societal Needs and Sensitivity to Disturbances

Societal needs reflect decisions about priorities, possible restrictions on civilian data transmission, etc. Effects on end-users from infrastructure failures are typically not linear with respect to damage to the infrastructure or to the amount of protection implemented (Johansson, Jonason Bjärenstam, and Axelsdóttir, 2018; Shield et al., 2021; UNDP and UNDRR, 2022). Typically, SCC failures have limited, short-term consequences for data communications but may cause restoration costs and uncertainty about reliability and governance. Proactive rerouting is critical primarily in specific situations or for certain high-priority data. Without information about such specific situations, suitable rerouting decisions cannot be made.

The SCC incident often creates substantial uncertainties about cause, reliability, and governance (Liebetrau and Bueger, 2024). Importantly, there is a low level of

secondary consequences of an incident, i.e., there is a low likelihood for cascading or escalating effects in the infrastructure and very limited environmental effects, etc. If there is a specific sensitivity to failure at a specific time and/or specific place, such information is important to protect. Therefore, proactive rerouting decisions are important only for specific conditions and for a limited amount of data of specific societal importance. Without information about such conditions, suitable rerouting decisions cannot be made.

Table 1. *Summary of the possible contributions of information that can be provided by different stakeholders in the maritime domain. Author created.*

Layer	**Contribution**
SCC0 technical status information	Unique and specific contribution to response to reduce consequences (reactive SA2).
SCC0 hazard and threat information	Specific and resource-efficient contribution to reduce likelihood and consequence (proactive and reactive SA2). Also contributes to learning and anticipation by giving information about the baseline activity and near misses (SA1 and SA3).
Maritime hazard and threat information	If combined with specific real-time underwater information: Contribution to anticipation (SA1), to learning and for reducing uncertainties (SA3), and to reduce likelihood and consequence (proactive and reactive SA2).
Independent infrastructure hazard and threat information (inspection)	Specific contribution to anticipation (SA1), but not feasible for real-time monitoring.
Military threat information	General contribution to anticipation (SA1), to learning and for reducing uncertainties (SA3).
Cyber threat information	General contribution to anticipation (SA1), to learning and for reducing uncertainties (SA3).
Hazard and threat information about alternative infrastructure	Central for balanced decision-making in response to reduce likelihood and consequence.

Assessment of societal needs and sensitivity to disturbances	Complex and context dependent, but crucial for balanced decision-making response to reduce likelihood and consequence.

Step 3: Evaluation of the Situational Awareness Created and the Possibility of Increasing Risk Mitigation and Resilience

An adequate capability must cover all three situational awareness components (SA1–SA3) in both the physical and cyber domains. Steps 1 and 2 above show that no single actor or layer of society can provide the information needed to create situational awareness. It is the combination of specific information about activities connected to SCC0 with general hazard and threat information, which creates value in terms of risk mitigation and resilience, provided that the information is actionable and suitable for decision-making.

Space-based alternatives offer diversity. However, overuse of alternative infrastructure decreases data communication quality (Jain et al., 2022) and space alternatives introduce capacity losses and sensitivity to new hazards and threats, possibly overshadowing the benefits of rerouting. Hence, rerouting decisions leveraging space-based infrastructure must be balanced, timely, and well informed by specific societal needs, ensuring reliable service for prioritised traffic.

Table 2 presents a summary of the prioritised contributions to each situational awareness component (SA1-SA3), and the findings are further elaborated in the text below.

Table 2. *Summary of the prioritised contributions to each situational awareness component (SA1-SA3). Author created.*

Situational awareness component	**Information, in order of contribution**
SA1: Information for anticipation	1. SCC0 hazard and threat information 2. Maritime hazard and threat information 3. Military threat information 4. Cyber threat information
Reactive SA2: Monitoring to provide information for reactive response	1. SCC0 technical status information 2. SCC0 hazard and threat information 3. Maritime hazard and threat information
Proactive SA2: Monitoring to provide information for proactive response	1. SCC0 hazard and threat information 2. Maritime hazard and threat information
SA3: Monitoring to provide information for learning and for reducing uncertainties	1. SCC0 hazard and threat information 2. Maritime hazard and threat information 3. Military threat information 4. Cyber threat information
Other information needed to support decision-making	1. Hazard and threat information about alternative infrastructure 2. Assessment of societal needs and sensitivity to disturbances

To create *situational awareness for anticipation (SA1),* the operator of SCC0 needs general cyber threat information and military-domain intelligence on hazards and threats to the infrastructure in question. As infrastructure hazards often change slowly but threat uncertainties can shift rapidly, anticipation must emphasise both physical and cyber threats, and operators must actively seek new information (Liwång, Sörenson, and Österman, 2015). However, anticipation is not merely about implementing adjustments but also about an organisational culture that acknowledges limited information (Lundberg and Johansson, 2015). Therefore, anticipation is dependent on the ability to look beyond the latest incidents and

understand that the introduction of a new threat does not necessarily reduce the risk related to old risks and hazards.

To create *situational awareness for response to reduce likelihood and consequence (SA2),* the operator needs specific and real-time information about the hazards and threats towards SCC0, preferably coupled with more general information about surface vessel traffic data in the vicinity of SCC0. Only then can proactive steps be taken to stop or limit an incident, warn end-users of imminent consequences, and prepare for rerouting to maximise the capacity and security of the new connection. Table 2 highlights that information suitable for active real-time physical response is limited. Therefore, physical protection needs to be implemented beforehand to provide for protection in case of accident or sabotage.

Central to the usefulness of monitoring is the ability to 'interpret the signs of an upcoming problem' (Lundberg and Johansson, 2015, p.26). Therefore, relevant and context-specific anomaly detection is central. Research on anomaly detection for ship traffic has been conducted (Relling et al., 2022), but additional classification of underwater events is needed to identify imminent hazards and threats to SCCs more precisely.

To successfully act on a problem and to coordinate resources, there need to be suitable response modes (Lundberg and Johansson, 2015). Moreover, any responses – such as rerouting – must also account for at least general information on societal needs and potential vulnerabilities. This requires the protection of sensitive information, as it includes details on military, public, and commercial aspects, as well as information about societal needs.

Multiple simultaneous infrastructure failures are a possible consequence of attacks carried out by threat actors with the intent of generating large-scale effects. This highlights the need for situational awareness that can detect synchronised or cascading incidents and ensure that decision-making is informed.

To create *situational awareness for learning and to reduce uncertainties (SA3),* the SCC operator must learn from its own incidents but, perhaps more importantly, be a part of a general societal process for learning, where stakeholders share information and

their assessments. Learning is central to resilience (Lundberg and Johansson, 2015) and is primarily a social aspect of the sociotechnical system. Such learning must address all the social aspects of the system, including governance and legal aspects. These aspects cannot therefore be assumed to be constant. An essential first step in implementing more efficient coordination among stakeholders could involve establishing information sharing and analysis focused on SCCs that bridges public and commercial actors. This public-private cooperation model could play a crucial role in fostering coordination among stakeholders in the domain of situational awareness. Such coordination and learning are also important for informing cable risk management to decide to what extent new cables should be buried and monitored for ensuring sufficient protection (Olsson, Franberg, and Kulesza, 2022).

As discussed in this study, effective situational awareness and consequent decision-making for SCCs rely not only on the proper integration of monitoring tools but also on coordination across the various actors of the network. The value of the information gathered about hazards and threats to a SCC may be greater for society than it is for the operator of the SCC. Also, significant heterogeneity often exists in how threats and failures are interpreted and addressed among different companies, as well as between the private sector and military stakeholders. These discrepancies can lead to delays and inefficiencies in the security of submarine communications and may be mitigated by bringing together diverse stakeholders to create a more shared risk understanding.

A well-balanced and implemented approach to SCC security increases the costs and risks of sabotage and decreases the impact of both accidents and sabotage. Additionally, appearing well protected is a deterrent and thus a protection in itself (Liwång, Sörenson, and Österman, 2015). However, across all areas identified, it is clear from this study that the resulting approach to SCC security is dependent on information about the weaknesses of the data communication system, as it is primarily the system functionality that needs to be protected, not the cable itself. For a commercial, nonstate operator of an SCC, contributing during crises or large-scale disturbances requires being recognised as a fully integrated defence stakeholder, e.g. having stronger links to relevant Navies and Coast Guards, with access to the information and threat intelligence necessary in this capacity. This affects how the SCC operator anticipates and learns as a defence actor, where the

operator's actions will have both civilian and military implications, and depends on the ability to integrate various types of risk intelligence to balance risks.

Discussion: Conditions for Balanced Rerouting

The conditions and need for rerouting of data communications vary by region, location, nation, and time. This constitutes both a technical and a social challenge. Rerouting is a core function of the data communication infrastructure. Therefore, critical maritime infrastructure protection is not focused primarily on the physical protection of the data communication system components. For society the focus should be on ensuring connectivity by redundancy, diversity, and decision-making that use the system's strengths. The more situational awareness is shared, the more decision-making can support resilience.

Space-based systems are not the only alternative to SCCs; aboveground microwave solutions could also provide an option that is independent of seabed hazards and threats. However, microwave solutions have range limitations as well as capacity challenges, and they introduce new weaknesses into the communication system.

If suitable possibilities for monitoring threats and risks to submarine communications infrastructure are implemented, they not only support governance and legal development but also strengthen the emergency functionality crucial for crisis management and military defence alike. For example, a more developed cross-disciplinary design and decision-making process would make it easier to implement prioritised crisis and military functionality directly fused into the infrastructure, e.g., implement military solutions for space-based back-up communication directly into the network instead of being stand-alone solutions. This, in turn, would increase the possibilities for alternatives in the event of a larger disturbance.

The investigations of this study open avenues for further development in technology, governance, and legal implications, as well as in how these aspects interact. However, for such a development, strategic aspects and the notion of sovereignty need to be further addressed by involved states. The interaction between technology, governance, and legal aspects is especially challenging given

the international and global characteristics of data communications compared with the national characteristics of defence and law.

There are also questions about the quality, fidelity, and feedback of the situational awareness discussed, as well as in relation to trust. For example, if the best information about threats and the critical need for continuous data communications exist in the military realm, while the capacity for long-distance data communications lies in the civilian and commercial realms, how should this complex interdependency between military and commercial organisations be arranged?

This study provides an understanding of possible contributions to SCC situational awareness and the appropriateness of their respective application to the operation of SCCs. The value of such situational awareness is supported by research in several different and independent fields. This normative and conceptual study generates new knowledge about the problem domain by outlining how the concept of situational awareness could be created and by prioritising different contributions. More applied work is needed to develop the specific processes, technology, and competencies that could contribute to more effective interactions between stakeholders in modern society's data communication systems.

Conclusion

This study takes a risk mitigation and resilience perspective by investigating the information needed to support decision-making. Appropriate situational awareness is dependent on general information about hazards and threats to feed into more continuous and long-term processes for anticipation and learning. However, decision-making is also dependent on specific information about hazards and threats targeting the cable in question.

A well-balanced and implemented approach to SCC security increases the costs and risks of sabotage and decreases the effects on society for both accidents and intentional attacks. However, across all areas identified, it is clear from this study that the resulting approach to SCC security is dependent on information about the weaknesses of the data communication system because it is primarily the system's functionality that needs to be protected, not the cable's functionality. Additionally, for a commercial nonstate operator of an SCC, such contributions to the system's

capability during crises or large-scale disturbances are not possible without being seen as an integral stakeholder of defence, and receiving the information needed to act in such a capacity.

Furthermore, this study highlights the importance of actively bridging civilian, commercial, and military interests through a shared operational framework. Such collaboration supports a holistic approach to hazard and threat identification, ensuring that physical and cyber vulnerabilities are addressed in tandem. By aligning technical capabilities with governance structures, stakeholders can more effectively anticipate emerging risks, enhance response measures, and ensure system-wide resilience.

While this study offers a conceptual and normative framework for improving submarine cable resilience, it does not provide empirical validation or detailed cost-benefit analyses. However, from the perspective of applied development, the conceptual capability perspective is often lacking, and resources and focus are placed on solutions with limited contributions to the capability needed.

Acknowledgements: We gratefully acknowledge the support from the NATO Science for Peace and Security (SPS) Programme to the Hybrid Space/Submarine Architecture Ensuring Infosec of Telecommunications (HEIST) research project. We also would like to thank participants at the HEIST 2024 workshop at Cornell University and the 2025 workshop at Blekinge Institute of Technology for fruitful discussions.

AI Statement: The Author(s) did not use Generative AI and/or AI-assisted technologies during the preparation of this work.

Works Cited

Adlakha-Hutcheon, G., Bin Hassan, F., Bown, F., Kivelin, J., Lindberg, A., Maltby, J.F.J., Molder, C., Peters, D.E., Rizzo, G., Roemer, S., Temiz, A., and Tocher, M. (2018) *A mid-way*

point on Futures Assessed alongside socio-Technical Evolutions (FATE) (DRDC-RDDC-2018-R211). Ottawa: Defence Research and Development Canada.

Andrews, J.D. and Moss, T.R. (2002) 'Common cause failures', in Andrews and Moss (eds.) *Reliability and risk assessment*. 2nd edn. London: Professional Engineering Publishing Limited, pp. 267-285.

Aven, T. (2009) 'Identification of safety and security critical systems and activities', *Reliability Engineering and System Safety*, 94(2), pp. 404-411. Available at: https://doi.org/10.1016/j.ress.2008.04.001.

Bakx, G.C.H. and Nyce, J.M. (2015) 'Risk and safety in large-scale socio-technological (military) systems: a literature review', *Journal of Risk Research*, 20(4), pp. 463-481. Available at: https://doi.org/10.1080/13669877.2015.1071867.

Bhatta, H.D., Costa, L., Garcia-Ruiz, A., Fernandez-Ruiz, M.R., Martins, H.F., Tur, M., and Gonzalez-Herraez, M. (2019) 'Dynamic measurements of 1000 microstrains using chirped-pulse phase-sensitive optical time-domain reflectometry', *Journal of Lightwave Technology*, 37(18), pp. 4888-4895. Available at: https://doi.org/10.1109/JLT.2019.2928621.

Boschetti, N. and Falco, G. (2025) 'Underwater cyber warfare: submarine communications cables architecture and cybersecurity analysis', *Proceedings of the 58th Hawaii International Conference on System Sciences*, 7 January. Available at: https://doi.org/10.24251/HICSS.2025.233.

Boschetti, N., Koyyada, A., Downs, B., Rosenthal, W., Gordon, N., Liwång, H., Marder, A., Sigholm, J., Frånberg, O., Kindgren, J., Frisk, T., Magnússon, B.M., Cavelty, M.D., Johnson, H., and Falco, G. (2025) 'Hybrid space and submarine architecture to ensure information security of telecommunications (HEIST)', *IEEE Access*. Available at: https://doi.org/10.1109/ACCESS.2025.3631359.

Brodkin, J. (2024) 'SpaceX tells FCC it has a plan to make Starlink about 10 times faster', *Ars Technica,* [online] 15 October. Available at: https://arstechnica.com/tech-policy/2024/10/spacex-claims-starlink-can-offer-gigabit-speeds-if-fcc-approves-new-plan/ (Accessed: 28 Jan 2025).

Bueger, C. and Liebetrau, T. (2021) 'Protecting hidden infrastructure: the security politics of the global submarine data cable network', *Contemporary Security Policy*, 42(3), pp. 391-413. Available at: https://doi.org/10.1080/13523260.2021.1907129.

Buzulukova, N. and Tsurutani, B. (2022) 'Space weather: from solar origins to risks and hazards evolving in time', *Frontiers in Astronomy and Space Sciences*, 9. Available at: https://doi.org/10.3389/fspas.2022.1017103.

Dansarie, M., Andersson, K.E., and Silfverskiöld, S. (2025) 'Crowd assessment of the military utility of future technologies', *Scandinavian Journal of Military Studies*, 8(1), pp. 200-219. Available at: https://doi.org/10.31374/sjms.339.

Duckworth, G., Owen, A., Worsley, J., and Stephenson, H. (2013) 'OptaSense distributed acoustic and seismic sensing performance for multi-threat, multi-environment border monitoring', *2013 European Intelligence and Security Informatics Conference*, pp. 273-276. Available at: https://doi.org/10.1109/EISIC.2013.70

Evans, J., Petillot, Y., Redmond, P., Wilson, M., and Lane, D. (2003) 'AUTOTRACKER: AUV embedded control architecture for autonomous pipeline and cable tracking', *Oceans Conference Record*, vol. 5, pp. 2651-2658.

Falco, G., Boschetti, N., Viswanathan, A., Bailey, B., Maple, C., Kurt, G.K., Willbold, J., Slay, J., Birrane, E., Logsdon, D., Bennett, S., Ferguson, W., Curbo, J., Oakley, J., Schloegel, M., Hagen, S., Sigholm, J., Mehlman, C., Thummala, R., Calabrese, M., Shah, Y., Le, A.T., Tan, K., Miller, E., Epiphaniou, G., Atmaca, U.I., Henry, W.C., Gür, G., Segate, R.V., and Yahia, O.B. (2024) 'Minimum requirements for space system cybersecurity – ensuring cyber access to space', *2024 IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, pp. 78-88. Available at: https://doi.org/10.1109/SMC-IT61443.2024.00016.

Furdek, M., Natalino, C., Di Giglio, A., and Schiano, M. (2021) 'Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats', *Journal of Optical Communications and Networking*, 13(2), p. A144. Available at: https://doi.org/10.1364/JOCN.402884.

Gordon, L.W. and Jones, K.L. (2022) *Global communications infrastructure: undersea and beyond*. Chantilly, Viriginia: The Aerospace Corporation, [online] Available at: https://csps.aerospace.org/sites/default/files/2022-02/Gordon-Jones_UnderseaCables_20220201.pdf (Accessed: 2 Jan 2025).

Grabis, J., Zdravkovic, J., and Stirna, J. (2018) 'Overview of capability-driven development methodology', in Sandkuhl and Stirna (eds) *Capability management in digital enterprises*. Cham: Springer International Publishing, pp. 59-84. Available at: https://doi.org/10.1007/978-3-319-90424-5_4.

Gutscher, M.-A., Quetel, L., Murphy, S., Riccobene, G., Royer, J.-Y., Barreca, G., Aurnia, S., Klingelhoefer, F., Cappelli, G., Urlaub, M., Krastel, S., Gross, F., and Kopp, H. (2023) 'Detecting strain with a fiber optic cable on the seafloor offshore Mount Etna, Southern Italy', *Earth and Planetary Science Letters*, 616. Available at: https://doi.org/10.1016/j.epsl.2023.118230.

Gutscher, M.-A., Royer, J.-Y., Graindorge, D., Murphy, S., Klingelhoefer, F., Aiken, C., Cattaneo, A., Barreca, G., Quetel, L., Riccobene, G., Petersen, F., Urlaub, M., Krastel, S., Gross, F., Kopp, H., Margheriti, L., and Beranzoli, L. (2019) 'Fiber optic monitoring of active faults at the seafloor: I the FOCUS project', *Photoniques*, pp. 32-37. Available at: https://doi.org/10.1051/photon/2019S432.

Hamilton, K. and Evans, J. (2005) 'Subsea pilotless inspection using an autonomous underwater vehicle (SPINAV): concepts and results', *Europe Oceans 2005*, vol. 2, pp. 775-781. Available at: https://doi.org/10.1109/OCEANSE.2005.1513154.

Hevner, A.R. (2007) 'A three cycle view of design science research', *Scandinavian Journal of Information Systems*, 19(2), pp. 87-92.

Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004) 'Design science in information systems research', *MIS Quarterly*, 28(1), pp. 75-105. Available at: https://doi.org/10.2307/25148625.

Howe, B.M., Angove, M., Aucan, J., Barnes, C.R., Barros, J.S., Bayliff, N., Becker, N.C., Carrilho, F., Fouch, M.J., Fry, B., Jamelot, A., Janiszewski, H., Kong, L.S.L., Lentz, S., Luther, D.S., Marinaro, G., Matias, L.M., Rowe, C.A., Sakya, A.E., Salaree, A., Thiele, T., Tilmann, F.J., von Hillebrandt-Andrade, C., Wallace, L., Weinstein, S. and Wilcock, W. (2022) 'SMART subsea cables for observing the earth and ocean, mitigating environmental hazards, and supporting the blue economy', *Frontiers in Earth Science*, 9. Available at: https://doi.org/10.3389/feart.2021.775544.

Jain, A., Patra, D., Xu, P., Sherry, J. and Gill, P. (2022) 'The Ukrainian internet under attack', *Proceedings of the 22nd ACM Internet Measurement Conference*, pp. 166-178. Available at: https://doi.org/10.1145/3517745.3561449.

Johansson, J., Jonason Bjärenstam, R., and Axelsdóttir, E. (2018) 'Contrasting critical infrastructure resilience from Swedish infrastructure failure data', in *Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*. Boca Raton: CRC Press, pp. 1287-1296.

Kessler, D.J., Johnson, N.L., Liou, J.C., and Matney, M. (2010) 'The Kessler syndrome: implications to future space operations', *Advances in the Astronautical Sciences*, 137(8).

Liebetrau, T. and Bueger, C. (2024) 'Advancing coordination in critical maritime infrastructure protection: lessons from maritime piracy and cybersecurity', *International Journal of Critical Infrastructure Protection*, 46. Available at: https://doi.org/10.1016/j.ijcip.2024.100683.

Liwång, H. (2017) 'Risk communication within military decision-making: pedagogic considerations', *Defense & Security Analysis*, 33(1), pp. 30-44. Available at: https://doi.org/10.1080/14751798.2016.1269389.

Liwång, H. (2022) 'Defense development: the role of co-creation in filling the gap between policy-makers and technology development', *Technology in Society*, 68. Available at: https://doi.org/10.1016/j.techsoc.2022.101913.

Liwång, H., Andersson, K.E., Bang, M., Malmio, I., and Tärnholm, T. (2023) 'How can systemic perspectives on defence capability development be strengthened?', *Defence Studies*, 23(3), pp. 399-420. Available at: https://doi.org/10.1080/14702436.2023.2239722.

Liwång, H., Ericson, M., and Bang, M. (2014) 'An examination of the implementation of risk based approaches in military operations', *Journal of Military Studies*, 5(2), pp. 38-64. Available at: https://doi.org/10.1515/jms-2016-0189.

Liwång, H., Sörenson, K., and Österman, C. (2015) 'Ship security challenges in high-risk areas: manageable or insurmountable?', *WMU Journal of Maritime Affairs*, 14(2), pp. 201-217. Available at: https://doi.org/10.1007/s13437-014-0066-9.

Lundberg, J. and Johansson, B.J. (2015) 'Systemic resilience model', *Reliability Engineering and System Safety*, 141, pp. 22-32. Available at: https://doi.org/10.1016/j.ress.2015.03.013.

Luu, M.A. and Hastings, D.E. (2022) 'On-orbit servicing system architectures for proliferated low-Earth-orbit constellations', *Journal of Spacecraft and Rockets*, 59(6), pp. 1946-1965. Available at: https://doi.org/10.2514/1.A35393.

Mauri, C. and Antonovsky, A. (2021) 'Using mixed methods to strengthen connections between human factors and complex socio-technical system', in *Proceedings of the 21st Congress of the International Ergonomics Association*. Cham: Springer, pp. 737-746. Available at: https://doi.org/10.1007/978-3-030-74602-5_100.

Milmo, D. (2025) 'Risk of undersea cable attacks backed by Russia and China likely to rise, report warns', *The Guardian*, [online] 17 July. Available at: https://www.theguardian.com/technology/2025/jul/17/risk-undersea-cable-attacks-backed-russia-china-likely-rise-report-warns (Accessed: 4 Nov 2025).

Möller, N. and Hansson, S.O. (2008) 'Principles of engineering safety: risk and uncertainty reduction', *Reliability Engineering and System Safety*, 93(6), pp. 798-805. Available at: https://doi.org/10.1016/j.ress.2007.03.031.

NATO NSO (2024) *NATO standard AJP-3.14 allied joint doctrine for force protection* (Edition B, v1). Brussels: NATO Standardization Office, [online] n.d. Available at: https://assets.publishing.service.gov.uk/media/672c8d4f62831268b0b1a2be/AJP_3_14_Force_Protection_EdB_V1-O.pdf.

NATO STO (2021) *Futures Assessed alongside socio-Technical Evolutions (FATE): final report of the SAS-123 Research Task Group*. Brussels: NATO Science and Technology Organization, [online] n.d. Available at: https://apps.dtic.mil/sti/pdfs/AD1148020.pdf.

Olsson, A., Franberg, O., and Kulesza, W.J. (2022) 'A new method for as-built burial risk assessment for subsea cables', *2022 2nd International Conference on Energy Transition in the Mediterranean Area (SyNERGY MED)*, pp. 1-6. Available at: https://doi.org/10.1109/SyNERGYMED55767.2022.9941457.

OX2 (2025) *Situational awareness at sea: a security concept for offshore wind and critical infrastructure*. Stockholm: OX2, [online] n.d. Available at: https://www.ox2.com/files/Sweden_documents/Summary_OX2_security_concept.pdf.

Potter, N. (2024) 'NATO's emergency plan for an orbital backup internet', *IEEE Spectrum*, [online] December. Available at: https://spectrum.ieee.org/undersea-internet-cables-nato (Accessed: 28 Jan 2025).

Relling, T., Lützhöft, M., Ostnes, R., and Hildre, H.P. (2022) 'The contribution of vessel traffic services to safe coexistence between automated and conventional vessels', *Maritime Policy and Management*, 49(7), pp. 990-1009. Available at: https://doi.org/10.1080/03088839.2021.1937739.

Roepke, W.-D. and Thankey, H. (2019) 'Resilience: the first line of defence', *NATO Review*, [online] 27 February. Available at: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html (Accessed: 09 Mar 2026).

Sherman, J. (2021) *Cyber defense across the ocean floor: the geopolitics of submarine cable security*. Washington, DC: Atlantic Council, [online] Available at: https://www.atlanticcouncil.org/in-depth-research-

reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/ (Accessed: 2 Jan 2025).

Shield, S.A., Quiring, S.M., Pino, J.V., and Buckstaff, K. (2021) 'Major impacts of weather events on the electrical power delivery system in the United States', *Energy*, 218. Available at: https://doi.org/10.1016/j.energy.2020.119434.

Sigholm, J. (2016) *Secure tactical communications for inter-organizational collaboration: the role of emerging information and communications technology, privacy issues, and cyber threats on the digital battlefield*. PhD thesis. University of Skövde, [online] Available at: https://fhs.diva-portal.org/smash/record.jsf?pid=diva2%3A1038714&dswid=8025.

Tärnholm, T. and Liwång, H. (2022a) 'Military autonomous underwater vehicles: an implementation perspective on legal and ethical aspects', *Journal of Maritime Research*, 19(3), pp. 39-46. [online] Available at: https://www.jmr.unican.es/index.php/jmr/article/view/660.

Tärnholm, T. and Liwång, H. (2022b) 'Military organisations and emerging technologies: how do unmanned systems find a role in future navies?', *Journal of Military Studies*, 11(1), pp. 37-48. Available at: https://doi.org/10.2478/jms-2022-0004.

Taweesintananon, K., Landrø, M., Brenne, J.K., and Haukanes, A. (2021) 'Distributed acoustic sensing for near-surface imaging using submarine telecommunication cable: a case study in the Trondheimsfjord, Norway', *Geophysics*, 86(5). Available at: https://doi.org/10.1190/geo2020-0834.1.

Tejedor, J., Macias-Guarasa, J., Martins, H., Pastor-Graells, J., Corredera, P., and Martin-Lopez, S. (2017) 'Machine learning methods for pipeline surveillance systems based on distributed acoustic sensing: a review', *Applied Sciences*, 7(8). Available at: https://doi.org/10.3390/app7080841.

Thodi, P., Paulin, M., Forster, L., Burke, J. and Lanan, G. (2014) 'Arctic pipeline leak detection using fiber optic cable distributed sensing systems', *OTC Arctic Technology Conference*, OTC-24589-MS. Available at: https://doi.org/10.4043/24589-MS.

Till, G. (2009) *Seapower: a guide for the twenty-first century*. 2nd edn. Abingdon: Routledge, pp. 286-321. Available at: https://doi.org/10.4324/9780203880487.

UNDP and UNDRR (2022) *Addressing the data gap: analysis of infrastructure damages and service disruption in PDNAs*. New York: United Nations Development Programme and United Nations Office for Disaster Risk Reduction, [online] Available at: https://www.undrr.org/publication/documents-and-publications/addressing-data-gap-analysis-infrastructure-damages-and (Accessed: 14 Oct 2025).

US GAO (2022) *Internet architecture is considered resilient, but federal agencies continue to address risks*. Washington, D.C.: United States Government Accountability Office, Information Technology and Cybersecurity, [online] Available at: https://www.gao.gov/products/gao-22-104560 (Accessed: 2 Jan 2025).

Wetter, O.E. and Wüthrich, V. (2015) '"What is dear to you?" Survey of beliefs regarding protection of critical infrastructure against terrorism', *Defense and Security Analysis*, 31(3), pp. 185-198. Available at: https://doi.org/10.1080/14751798.2015.1056941.

Wills, S. (2020) "'These aren't the SLOC's you're looking for": mirror-imaging battles of the Atlantic won't solve current Atlantic security needs', *Defense and Security Analysis*, 36(1), pp. 30-41. Available at: https://doi.org/10.1080/14751798.2020.1712029.

Winter, R. (2008) 'Design science research in Europe', *European Journal of Information Systems*, 17(5), pp. 470-475. Available at: https://doi.org/10.1057/ejis.2008.44.

Yue, Y. and Henshaw, M. (2009) 'An holistic view of UK military capability development', *Defense and Security Analysis*, 25(1), pp. 53-67. Available at: https://doi.org/10.1080/14751790902749900.