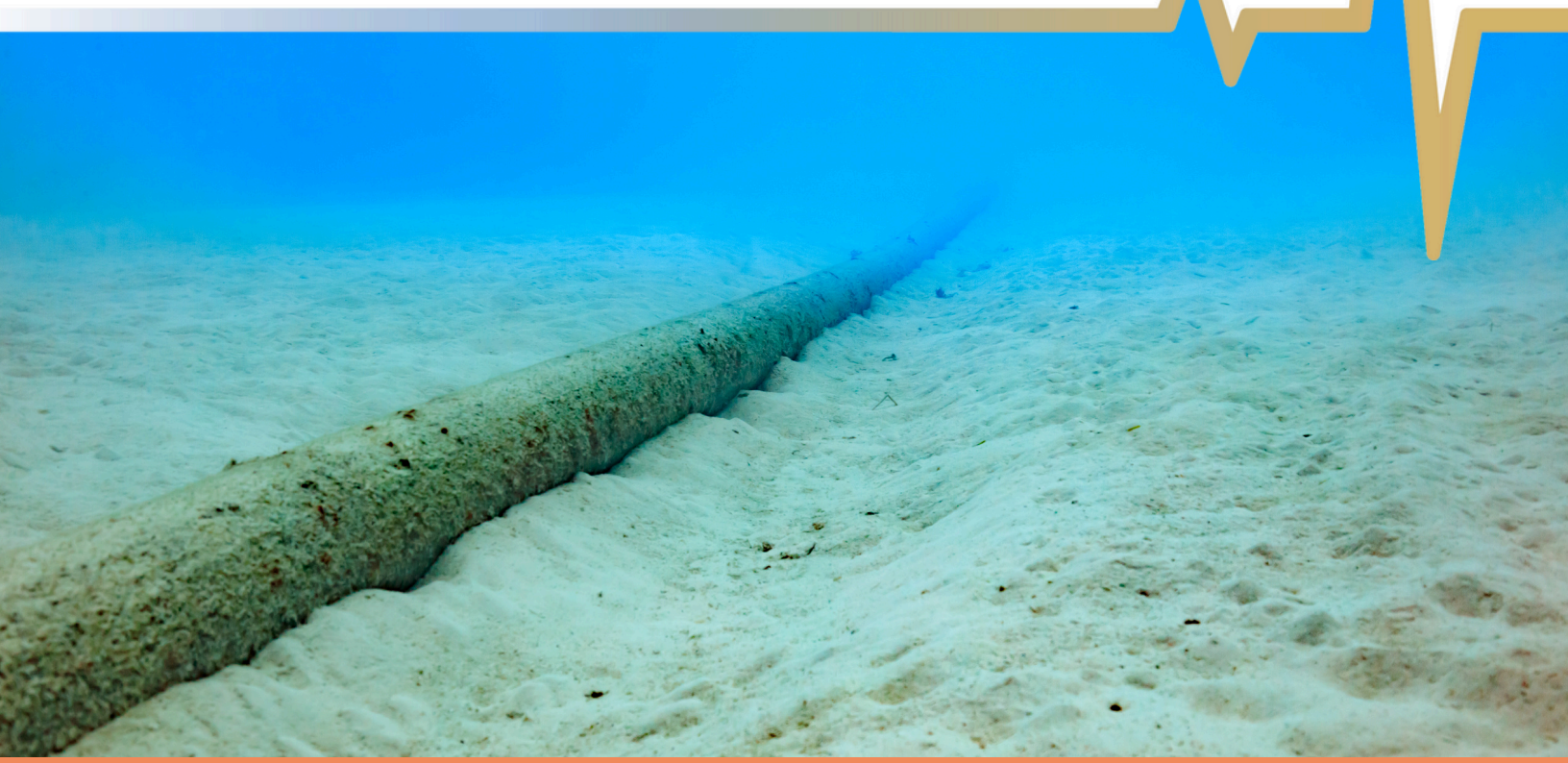
Cross-Sector Impacts of Subsea Cable Disruptions on Critical Infrastructure

TLP:WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.



Health-ISAC® Collaborating for Resilience in Health
SPACE ISAC
E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Key Judgements

- Subsea cables play a key role in modern interconnectivity, but also represent a vast unmonitored attack surface for threat actors seeking to cause disruptions.
- Deliberate attacking of subsea cables to cause disruptions has been observed in hybrid warfare campaigns.
- Damage to subsea cables can result in power and telecommunication outages for critical infrastructure organizations.
- Subsea cable disruptions that do not directly affect critical infrastructure owners may impact critical third parties, resulting in sudden supply chain delays.
- Scenario-based risk planning exercises, also known as table-top exercises (TTXs), can be an effective way to develop and stress-test business resilience plans in the event of a sudden utility outage.

Introduction

Subsea cables are considered to be an integral part of modern interconnectivity. According to the US policy think tank, the Center for Strategic and International Studies (CSIS), approximately 95% of information shared across continents is done along undersea cables[1]. However, certain geopolitically motivated events have shifted the status quo, placing these cables at heightened risk. During the onset of the Russia-Ukraine war in 2022, the subsea liquid natural gas pipelines running from Russia to Germany were severely damaged using underwater explosives during a tense political battle over EU sanctions on Russian liquid natural gas. This highlighted the volatility of critical subsea infrastructure.

Critical infrastructure, such as subsea cables, underpins vital roles of communication across multiple segments and layers. For example, satellite system operations are directly dependent on subsea cable data transmission and vice versa. Terrestrial-based telecommunication and network services directly rely on subsea cables for the rapid transmission of data. Subsea cables transport tremendous amounts of data, but when a cable disruption event occurs, this data must be rerouted immediately, putting increased strain and stress on other cables, terrestrial-based infrastructure, and broadband satellites. This becomes a potential time for adversaries to strike through a multitude of attack vectors via both kinetic / non-kinetic methods.

1. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Attribution towards sabotage of subsea cables is difficult to prove as investigations can often take months – years to complete, yielding no viable evidence found. Nonetheless, since Russia's full-scale invasion of Ukraine on 24 February 2022, subsea cable disruption events in the Baltic Sea / Gulf of Finland have increased, as noted by events impacting cables connecting infrastructure between Finland and Estonia[2], and Sweden and Lithuania[3]. Similarly, as geopolitical tensions between China and Taiwan continue, there are subsequent targeting of subsea cables as Taiwan has officially ruled sabotage was at play as a Chinese vessel Shunxin-39 was officially recognized as maliciously damaging a subsea cable in January 2025[4]. Moreover, Yemen-backed Houthi Rebels have been officially recognized as damaging subsea cables in the greater Arabian Sea area in March 2024.[5]

Cross-Sector Considerations

Subsea cables are an integral part of modern critical infrastructure, connecting cities and countries. While the number of cables serving a given location varies significantly, the impact of a major subsea cable disruption could result in prolonged power outages and telecommunication outages for critical infrastructure owners. Below, Health-ISAC, Space-ISAC, and E-ISAC have summarized the possible impacts of a telecommunications or energy outage brought on by subsea cable disruptions on their respective sectors.

Impacts of Subsea Cables on the Health Sector

The impact of utility outages on the health sector can cause patients to be unable to receive the treatment or medicine they need, sudden appointment rescheduling and other impacts that hinder patients from obtaining care. This risk is further compounded by the growing trend of telecommunication adoption in the patient delivery ecosystem. Now, internet or other telecommunication outages can result in a loss of care for patients as well.

One of the systemic risks to utility outages in health sector organizations bordering large bodies of water is the subsea infrastructure facilitating the flow of information and electricity. Because of their reach, subsea cables are considered to be an integral part of modern interconnectivity. According to the US policy think tank, the Center for Strategic and International Studies (CSIS), approximately 95% of information shared across continents is done along undersea cables[6]. Therefore, these cables are absolutely critical to the flow of information across large bodies of water like oceans or seas. In the context of healthcare, this translates to access to electronic health records (EHR) and protected health information (PHI) for global organizations, both of which are vital to ensuring patients get the most optimal care possible.

2. https://www.cbsnews.com/news/finland-undersea-cables-sabotage-russia-linked-ship-dragged-anchor/
3. https://www.cnn.com/2024/11/18/europe/undersea-cable-disrupted-germany-finland-intl/index.html
4. https://fmso.tradoc.army.mil/2025/taiwan-suspects-chinese-ship-of-cutting-undersea-data-cables/
5. https://apnews.com/article/red-sea-undersea-cables-yemen-houthi-rebels-attacks-b53051f61a41bd6b357860bbf0b0860a
6. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Telecommunication Outage

In the event that a health sector institution loses its ability to connect to the internet, it could lose access to electronic health records, making it much harder to provide care to patients. One such case where the loss of telecommunication to a health sector organization caused cascading consequences was the ransomware attack against the Southeastern blood donation organization One Blood. Once the systems were inaccessible, the blood donation organization had to use pen and paper to label each sample manually, which slowed down the distribution process to the point where they advised all 250 hospital customers to activate critical blood shortage protocols.[7]

In fact, when telecommunication outages impact critical third-party suppliers, the resulting shortages can linger far after the incident has been remediated. In 2024, a blood plasma supplier in the UK, Synnovis, was hit with a ransomware attack in June 2024, preventing access to patient EHR. This resulted in thousands of O-negative and O-positive blood donations to be destroyed because it was too difficult to rapidly identify a patient's blood type without access to EHR. This attack caused the NHS Blood and Transplant (NHSBT) body to issue a blood shortage amber alert. In June 2025, about a year later, the Amber Alert is still in effect. NHS is calling for an additional 200,000 blood donors to increase the supply of O-negative blood to offset the damage done by the attack in 2024.[8]

Another example of the dependency the modern health system has on reliable telecommunication was when a large patient care authorization software went down after a ransomware attack in 2024. This outage was massively impactful, with physicians not being able to authorize care for patients and pharmacies being unable to process prescription payments. The payment portal handled an estimated 15 billion transactions every year, and its outage forced some patients to pay full price for medication and treatment, or forced them to postpone treatment until the software was operational again.[9]

Power Outage

Similarly, the Health Sector is dependent on a steady supply of energy to power medical equipment and maintain sanitary environments. In the absence of power, a hospital's effectiveness in caring for its patients diminishes significantly. In a tragic example, the Memorial Medical Hospital in New Orleans was without power for five days in the aftermath of Hurricane Katrina in 2005.

7. https://www.miamitimesonline.com/lifestyles/health_wellness/florida-hospitals-face-blood-shortage-after-cyberattack/article_e2cb7312-5427-11ef-b56d-dfaa9a055153.html
8. https://www.thesun.co.uk/health/35320931/nhs-urgent-call-blood-donors-critical-emergency-stocks-low/
9. https://www.hipaajournal.com/change-healthcare-ransomware-attack-having-massive-impact-on-providers/

During this incident, a massive flood occurred that destroyed backup generators and caused a total outage. This increased the internal temperature of the hospital beyond 100° Fahrenheit (38° Celsius). The hospital remained in this isolated state for five days before evacuation from August 28 to September 1, 2005. Memorial Medical Hospital was left without power, lights, sewer systems, and air conditioning. Medical equipment was rendered inoperable. Evacuation was impossible as the bottom floor of the building was flooded, preventing egress. When faced with this daunting situation, physicians and staff adopted an unorthodox method of medical triage in which the critically ill patients with do-not-resuscitate (DNR) orders were deprioritized.[10]

Impacts of Subsea Cable Disruptions on the Space Sector

Subsea Cables and Ground Station Dependency:

Submarine communication cables (SCCs) connect data centers, cloud centers, landing stations, and satellite ground stations together.

***Image 1**: SSCs and Satellite Ground Networks in Northern Europe*[11]

A cyberattack or sabotage of the existing SCCs, landing stations, and satellite ground stations would compromise the multi-source / multi-path data fusion delivery between satellites and SCCs. These sources are integral to Space Situational Awareness / Space Domain Awareness for mission planning and protection of critical assets both on-orbit and at the terrestrial layer. For example, the Svalbard SCC has been developed to allow for the expansion and upgrade of the Svalsat satellite ground station complex located within the Arctic Circle. The Svalbard SCCs and ground stations are one of the primary confluences of the KSAT global ground station network. Northern Europe within the Arctic Circle has become increasingly diversified in terms of satellite stations, data centers, and adversarial nations looking to extend their presence. Satellite stations / data centers of Microsoft, Amazon Web Services, Swedish Space Corporation, and KSAT are all located in this area.

10. https://www.eonline.com/news/1341588/the-harrowing-true-story-behind-five-days-at-memorial
11. https://www.researchgate.net/publication/388420509_Underwater_Cyber_Warfare_Submarine_Communications_Cables_Architecture_and_Cybersecurity_Analysis

A malicious cyberattack or physical disruption on any one of these SCCs, landing stations, ground stations, etc. can prove vital. Moreover, assets at these higher latitudes must contend with impacts derived from Space Weather, as power grid fluctuations and increased ionospheric scintillation can put both at risk of disruption.

Subsea Cables and Satellite Dependency:

SCCs face risks from geopolitical tensions while satellites face potential risks from anti-satellite weapons. In conjunction, a host of malicious cyber threat activity exists for the intermediaries between the two assets.[12] The ViaSat cyberattack at the onset of the Russian-Ukraine war highlighted the critical vulnerabilities in satellite systems. In turn, Low Earth Orbit (LEO) satellites have introduced a new synergy with SCCs that highlight the critical dependency both rely on.[13] LEO satellites offer advantages such as global reach, reduced latency, and enhanced resiliency.[14] Still, both are dependent on one another considering an attack or disruption. When the Intelsat 33e satellite broke up in geostationary orbit, over seven nations were directly impacted as SSCs had to reroute data[15]. Nearly 20 nations experienced degraded services, whereas Telecom Namibia couldn't fully restore their Very Small Aperture Terminals until nearly three months later.

Correlation of GNSS Interference and Subsea Cable Outages:

When there is a subsea cable disruption event that occurs globally, it is routinely consistent with some form of Global Navigation Satellite System (GNSS) interference, jamming, or spoofing. This is a direct attempt to disrupt, deny, degrade, and damage satellite systems by dispelling harmful interference signals into the ionosphere. Observations of harmful interference events impacting satellite systems in conjunction with targeting subsea cables directly highlight a multitude of SPARTA Tactics, Techniques, and Procedures. These include jamming, spoofing, position, navigation, & timing Geofencing, deception (or misdirection) and more. Impacts are evident across multiple flight and maritime captures of these vehicles operating near the impacted corridors when a subsea cable is damaged.

12. https://bisi.org.uk/reports/strategic-alliance-of-sea-and-space-synergies-between-subsea-cables-and-leo-satellites
13. https://xonapartners.com/wp-content/uploads/2020/12/Defining-the-Synergies-between-LEO-Satellite-Constellations-and-Submarine-Cables.pdf
14. https://www.linkedin.com/pulse/subsea-cables-vs-satellite-future-balancing-act-almerindo-%C3%A1zera-stimf/
15. https://www.linkedin.com/pulse/subsea-cables-vs-satellite-future-balancing-act-almerindo-%C3%A1zera-stimf/

Impacts of Subsea Cable Disruptions on the Energy Sector

Submarine Power Cable Overview

While most subsea cable infrastructure is related to communications, a small minority are power cables used in the energy sector. These include cables connecting offshore energy infrastructure with power for operations; offshore renewable energy infrastructure (such as wind turbines) remitting their generated power back to shore; and connections between generation, transmission, or distribution assets over bodies of water.[16] The latter type includes not only intranational interconnections such as the cable connecting the island of Crete with mainland Greece, but international cooperative interconnections such as the North Sea Link between Norway and the United Kingdom. Examples of subsea cables used in North America include cables connecting Long Island, New York, to the U.S. mainland, the Hudson Transmission Project's subsea cable connecting New Jersey to Manhattan, as well as similar cables connecting Vancouver Island, Newfoundland and the Labrador Peninsula to mainland Canada. Most other active subsea power cables in North America are used to transmit power from offshore wind farms off the U.S. East Coast.

Power Outage

North America's subsea power cable footprint is significantly smaller than that of Europe and is less vulnerable to physical attacks aimed at disrupting the electric grid. Severance of North American subsea cables could lead to significant localized electric grid disruptions, including power shortages, but widespread, sustained outages might be avoided in such cases due to local backup power and generation and transmission sources which do not rely on subsea power cables.[17]

Submarine power cables carry many of the same risks as submarine telecom cables. Foremostly, submarine power cables are typically laid alongside telecom cables on the seafloor and often inhabit the same seafloor features (natural or artificial trenches, for example). Some subsea cables are also "hybrid cables" combining different types of conductors with optical fibers within a single cable to transmit power, data, and potentially other signals.[18] As a result, certain forms of accidental damage (including anchor or fishing activity as well as natural events like underwater earthquakes and landslides) or intentional sabotage of submarine telecom cables can often risk impacting power cables as well[19]. Additionally, both types of cables often rely on many of the same vendors for materials, maintenance, and cable laying services, creating a shared nexus of cybersecurity risk from the breach of these vendors for both the telecom and energy sectors.

16. https://www.globalgrowthinsights.com/market-reports/subsea-power-cable-market-105848
17. North American Electric Reliability Corporation (NERC) Bulk Power System Awareness (BPSA)
18. https://www.subseacables.net/reports-and-coverage/transforming-global-connectivity-with-submarine-hybrid-power-telecom-cables/
19. https://ultramapglobal.com/the-biggest-threat-to-subsea-cables/

The differences between submarine power and telecom cables, however, carry security implications. In most cases, submarine telecom cables are smaller and less expensive than submarine power cables. Typically, resiliency in submarine telecom cables can be shorn up via a redundancy of cables – laying numerous cables in a single location with multiple interconnection nodes so that damage to a single cable can allow telecom traffic to reroute through another. Doing so with submarine power cables can be more cost-prohibitive, so some submarine power cables lack redundant connections, making cuts or damage more impactful.

Deliberate physical sabotage by state-linked actors (as part of a hybrid warfare strategy) has been used to attack subsea cables in the past.[20] One such incident occurred on December 25, 2024, when the Estlink 2 subsea power cable connecting Estonia and Finland failed due to suspected sabotage by a Russian-linked vessel dragging its anchor.[21] Although cross-border power transmission was reduced significantly, there were no reports of outages due to this incident.[22] Finnish media at the time reported that the repairs were expected to take up to seven months and cost tens of millions of Euros.[23]

Telecommunication Outage

North America's electric grid also has limited exposure to risks from subsea telecommunication cable severance, given the fact that much of the internet traffic that electricity sector sites rely on for monitoring Supervisory Control and Data Acquisition (SCADA) systems, energy market transactions, and inter-utility coordination, is intranational and not international in nature. This traffic is typically routed through terrestrial fiber networks or microwave/satellite links. Some exceptions to this can be found for coastal, offshore or island-based grid assets which rely on subsea telecommunication cables to connect to mainland control centers, though these represent limited utility exposure in North America. Certain energy sector vendors provide cloud-based services (analytics or electricity demand forecasting, for example) and this traffic is more likely to rely on subsea telecommunication. In the event that a communication outage occurs at electricity sector sites, backup communications such as microwave and satellite links can be relied on to help mitigate the impact.

19. https://ultramapglobal.com/the-biggest-threat-to-subsea-cables/
20. https://www.reuters.com/world/europe/poland-says-russian-ship-performed-suspicious-manoeuvres-near-cable-sweden-2025-05-21/
21. https://www.bbc.com/news/articles/c1elq7lx9qdo
22. https://www.reuters.com/world/europe/finland-investigates-outage-undersea-power-link-estonia-finnish-pm-says-2024-12-25/
23. https://www.mtvuutiset.fi/artikkeli/estlink-2-kaapelin-korjaustyot-tulevat-maksamaan-kymmenia-miljoonia/9074298

Mitigation Strategies:

To minimize the risk of subsea cable disruptions leading to high-impact events, critical infrastructure owners can take the following measures:

- **Table Top Exercises** - participate in scenario-based risk discussions, also known as tabletop exercises (TTXs), that center around sudden power or telecommunications outages. This will help organizations develop and implement business continuity strategies.
- **Utility Redundancy** - In the event that a communication outage occurs at electricity sector sites, backup communications such as microwave and satellite links can be relied on to help mitigate the impact. Backup generators that run on petrol or another independent fuel source may be a valuable contingent measure to minimize the impact of a sudden power outage.
- **Identify Supply Chain Pain Points** - readers are encouraged to go through their supply chain to identify elements that may be highly reliant on subsea infrastructures and determine equities, dependencies to include relationships that would help clarify the supporting versus supported relationships traversing these critical conduits thereby contributing to risk & resiliency considerations.

Conclusion

Subsea cables play a unique role in global connectivity, especially as critical infrastructure services adopt more digitization measures. While this benefits the consumer by streamlining access and boosting innovation, threat actors seeking to engage in gray-zone warfare, disruptive attacks that fall just below the threshold of kinetic conflicts, may target subsea infrastructure due to the potential impacts and immense attack surface. As this threat vector evolves, forward-facing threat intelligence consumption is a crucial part of staying ahead of the curve. Such intelligence can be found in open-source news reporting, blog posts from intelligence vendors, and information-sharing communities.

Subsea cables are just one of many threat vectors facing critical infrastructure. Due to the growing interdependence of the critical infrastructure ecosystem, a collective approach to security has become necessary. Information-sharing communities can be an essential component in staying abreast of emerging security trends. Communities like the ISACs allow members to become informed about evolving security risks due to the availability of multiple informed perspectives offering sector-specific insights.