Cyber Security in the Subsea Telecommunication Cable Networks

Martti Lehto[1], Petro Julkunen[2] and Hans Hartikainen[1]
[1]Faculty of Information technology, University of Jyväskylä, Finland
[2]Department of Technical Physics, Faculty of Science, Forestry and Technology, University of Eastern Finland, Kuopio, Finland

martti.lehto@jyu.fi
petro.julkunen@uef.fi
hans.k.hartikainen@jyu.fi

Abstract: More than 95% of international internet and telecommunication data is transmitted through subsea fiber-optic cables, valued for their cost-efficiency, low latency, and high capacity. The cables connect the network of data centers around the world to form our internet. This physical infrastructure is critical to the modern world as most modern services depend on it. There are currently over 550 commercial subsea telecommunication cables in-service and many more planned or being constructed. It is crucial to provide resilience of the subsea cables against environmental, human, and other activities that may break any one or multiple cables. Despite their critical importance to global communications, these vast networks remain vulnerable to a range of cyber threats. The remote location of subsea cables does not preclude risks; rather, their endpoints, landing stations, and network management systems are susceptible to malicious actors seeking to intercept, disrupt, or manipulate data flows. As international reliance on these information systems increases, so does the strategic imperative to secure them against espionage, sabotage, and emerging cyber-attacks. Successful cyber-attacks are predicated on exploiting system vulnerabilities. Vulnerability can be defined as exploitable weaknesses or deficiencies in a system, device or its design that allow cyber attackers to execute cyber-attacks. A weakness in system security procedures, software applications, policies and procedures and regulatory compliance may be caused by vulnerabilities. The inherent weakness in the system caused by vulnerability increases the probability of a harmful occurrence or exacerbates its consequences. Vulnerabilities can be divided into those that exist in people's actions, processes in the organizations, and technologies. The paper discusses cyber vulnerabilities, threats and management thereof in the telecommunications network.

Keywords: Subsea cable, Vulnerability, Cyber-attack, Cyber security

1. Introduction

Threat, vulnerability, and risk form an intertwined entirety in the cyber world. Vulnerability can be defined as an exploitable weakness or deficiencies in a system, device or its design that allow threat agents/actors to execute illegal actions in the target system. The paper analyzes vulnerabilities among cable operators and vulnerabilities related to cable technology and IT/OT/SCADA systems (software & hardware).

A cyber threat compiles information related to potential cyber threats targeting various entities such as a system, enterprise, System of Systems (SoS), region, or a critical infrastructure sector. This model serves as a foundational element for diverse tasks across different scopes. Achieving comprehensive cyber security necessitates a thorough analysis of a system of systems (or sub-system) against a spectrum of threat events.

Defining threats within the cyber space realm presents challenges, primarily due to the elusive nature of attack origins, the intricate motives driving them, and the unpredictable unfolding of events. The complexities are further heightened by the blurred boundaries between national, international, public, and private interests, exacerbated by the global nature of cyber threats and the rapid evolution of technology.

Small countries, such as many European nations and island nations that have limited cable access points, are vulnerable to cyber-attacks on the cables, which could have widespread disruptions that go beyond the immediately targeted nation or region as the cables are part of larger networks. Depending on the motivation of the threat actors, the vulnerable points within the cable network may vary. (ODNI, 2017; Gallagher & Carter, 2023)

This paper describes the findings of a research project that examined cyber threats targeting Critical Subsea Infrastructure (CSI). The study focuses on PPT (People-Processes-Technology) vulnerabilities in CSI. The paper outlines the cyber threat environment, identifies vulnerabilities to PPT, and estimates potential impacts. This study consists of conducting a system description, cyber threat analysis, vulnerability analysis, cyber-attack model analysis and impact analysis.

2. System of System Description

A system of systems (SoS) is a collection of systems, each capable of independent operation, that interoperate together to achieve additional desired capabilities. The SoS concept describes the integration of many

independent, self-contained systems to satisfy needs of the organization. The synthesis of these very large systems often results in different problems than those presented by the design of a single, yet complex, system.

2.1 Undersea Cable Network

The architecture of a typical subsea telecommunication cable network is divided into elements of wet plants and dry plants with cable landing stations (CLSs), beach manholes, subsea cables, and repeaters, gain equalizers, amplifiers and branching units. The subsea communications cable connects the landing station which houses the subsea line terminal equipment, where the subsea telecommunication cable is divided into the optical fiber and the power supply line. (Julkunen, 2025)

Amplifiers and repeaters are both components that enhance the signal in order to mitigate the amplitude loss over extended distances. Repeaters are placed "in-line" (placed in intervals along the cable) and amplifiers "off-line" (placed at the end of the cable run). (Chesnoy, 2016)

2.2 Telecommunication Cable

An undersea cable's structure consists of a central bundle of glass optical fibers for data transmission, surrounded by multiple layers of protective materials, including gel, a copper conductor for power, steel strength members for structural integrity, and a robust outer jacket made of polyethylene, nylon, and additional steel wires or aramid yarns. Repeaters are strategically placed along the cable to amplify weak light signals over long distances, and cable landing stations are where the undersea cables connect to terrestrial networks. The constituents of the cable itself, listing from the center outwards, are first, the data-carrying optical fibers and core, strength wires, copper sheath to power the underwater equipment, insulation jacket, followed by varying amounts of protective layers. (Chesnoy, 2016)

2.3 Supervisory Control and Data Acquisition

A key component of critical infrastructure is operational technology (OT), which includes the most important ones: Industrial Control System (ICS), Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS) and Programmable Logic Controller (PLC). These systems are key components of the subsea cable network. SCADA consists of physical and software components, which include sensors and actuators, data transmission networks, controllers, communication devices, user interface (HMI) and software. (Lehto, 2022; Hartikainen, 2025)

3. Stakeholders in the Subsea Cable Network

The owners invest in subsea cables/pipelines to increase the capacity for meeting the demand or to expand coverage to serve new regions and customers. Telecommunication cables are often owned and installed by private companies such as telecommunication carriers or subsea cable companies but can also be state-owned. Ownerships can also be distributed instead of a single owner to consortiums or public-private partnerships (Reverdy & Skenderoski, 2015).

Suppliers for subsea telecommunication systems include companies that are fully integrated system suppliers, system integrators, cable suppliers, Subsea Line Terminal Equipment (SLTE) suppliers, and special component suppliers. The suppliers often have access to the cables and pipelines for construction, repairs and maintenance, and possess a deep know-how on the systems as well as proper hardware and the ability to analyze and repair damage.

The stakeholders include governments, organizations and people connected via the subsea cables and pipelines, and potentially those with financial and strategic interests in those connections, regional or global. The operators and stakeholders are intertwined and connected as presented in Figure 1. The connections are generated by the operators' and stakeholders' interdependencies and their resources and assets. (Gallagher & Carter, 2023; Julkunen 2025).

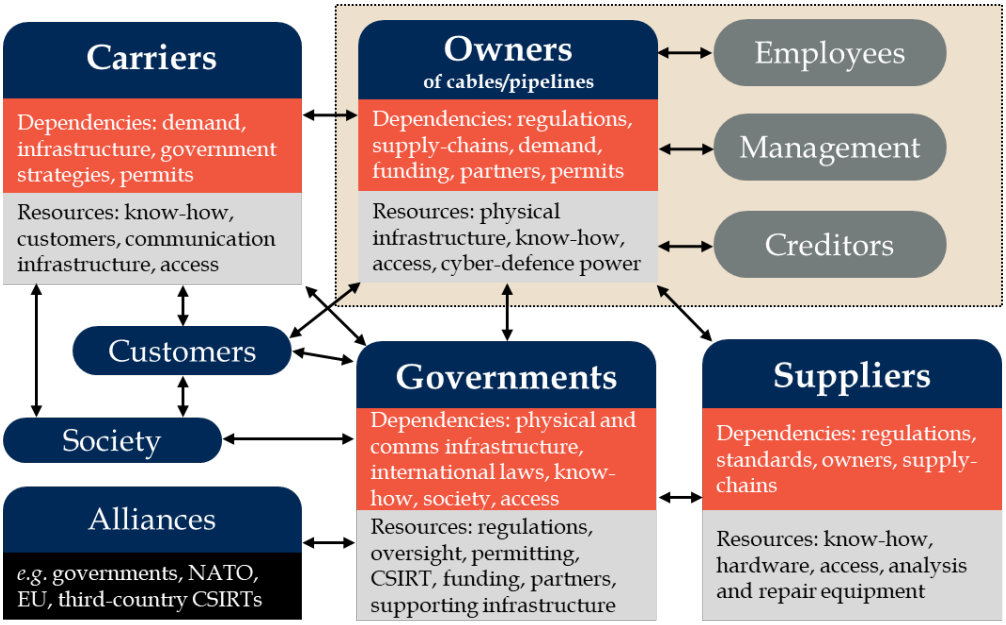

Figure 1: Network of operators and stakeholders

The people of the operator cable/pipeline operator organizations include the employees, management, potential consultants and subcontractors, as well as investors and auditors. These people are considered to have access that exceeds that of a person operating outside of the organization. These people are hence important concerning limiting access to cables and pipelines, and the associated systems including the software and hardware and monitoring systems, like SCADA. Hence, the cable/pipeline organizations and their safety are dependent on the cyber security skills and know-how of the people in those organizations as well as the level of understanding on cyber security. The people in those organizations generate processes initiated by internal or external motivation.

An insider is a cyber-attacker who has legitimate access to the organization and its knowledge and resources. (UK-NCSC, 2022) Also ENISA considers also human errors and carelessness to be included. (ENISA, 2024) While the motivation of insiders can broadly fit in with our wider taxonomy, they are a special category warranting consideration. Empirical results suggest main motivations for insider cyber sabotage to be revenge, personal gain, poor performance and addiction. (Maasberg et al., 2020) Most prevalent insider incidents are fraud (44%), sabotage (24%) and intellectual property theft (16%), with miscellaneous (12%) and multicategory (4%) making up the rest. (Collins, 2013)

4. Threat Analysis

Threats in cyber space are difficult to define due to challenges in defining the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public, and private interests. Because threats in cyber space are global and involve rapid technological developments, the struggle to counter them is ever-changing and increasingly complicated. (Lehto, 2022)

For this study, a practical threat taxonomy based on the motivation of the attacker has been developed. The threats included in the suggested threat model are all applicable to the critical infrastructure assets presented in the chapter. The presented threat taxonomy mainly covers cyber security threats; that is, threats applying to the whole OT environment.

A common threat model is a six-fold classification based on motivational factors: cyber vandalism, cybercrime, cyber intelligence, cyber terrorism, cyber sabotage, and cyber warfare. The motivation also affects the attacker's targeting and methods. While a terrorist seeks visibility, a spy wishes to stay unnoticed to gain information. Different attacker archetypes (Table 1) also have different triggers, i.e. events or conditions that cause the attacker to execute the attack.

Table 1: Cyber threat adversary archetypes' attributes

	Vandalism	Crime	Intelligence	Terrorism	Sabotage	Warfare operations
Motivation and goal	Pursuit of changing the environment or cause harm. *Egoism*	Pursuit of financial gain *Financial*	Pursuit of information to support decision-making. *Information*	Pursuit of social instability and influencing political decision-making. *Anarchy*	Pursuit of instability, chaos, political change, infrastructure paralysis. *Paralysis*	Pursuit of paralysis/destruction of nation's digital infrastructure. *Political or military dominance.*
Target	Digital services of the governments, companies, and citizens' information systems.	Digital services of the governments, companies, and citizens' information systems.	Data and information of governments, companies, important individuals	Data and information of governments, companies and critical infrastructure.	Nation's critical infrastructure.	Nation's critical infrastructure (civilian or military).
Attackers' capability	Acquired	Augmented	Advanced	Advanced	Integrated	Integrated
Impacts	Disruptions in digital services	Financial losses	Data and information loss	Disruptions and paralysis in digital services and critical infrastructure	Paralysis and damage in critical infrastructure	Paralysis, damage and destruction in critical infrastructure

5. Vulnerability Analysis

Threat, vulnerability, and risk form an intertwined entirety in the cyber world. Vulnerability can be defined as an exploitable weakness or deficiencies in a system, device or its design that allow cyber-attackers to execute cyber-attacks. Vulnerabilities may be the outcome of a weakness in system security procedures, software applications, policies and procedures and regulatory compliance. Vulnerabilities are inherent weaknesses in the system which increases the probability of an occurrence or exacerbates its consequences. (Lehto, 2022)

Vulnerabilities can be divided into those that exist in people's actions, processes in the organizations, and technologies.

People refer to the human resources available at the firm's disposal. The people are the ones who do the tasks described in the process. Employees are often victims of social engineering tactics and may end up unknowingly providing attackers with login credentials or classified organization data. (Lehto, 2022)

Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information. Process vulnerabilities among others are lack of written security policy, poor regulating policy, lack of security awareness and training, and poor adherence to security, lack of access control and non-existence of disaster/contingency plan.

Technology solutions protect against cyber risks that may arise from network vulnerabilities, but technology itself contains vulnerabilities (hardware, HW and software, SW). So, technological vulnerabilities are security holes in a system. (Hartikainen, 2025)

Vulnerabilities concerning people and processes in cyber security of critical subsea infrastructure. The operational vulnerabilities, i.e. vulnerabilities associated with human action and processes. The entire vulnerability scene of the cyber space of critical subsea infrastructure has been summarized in Figure 2.

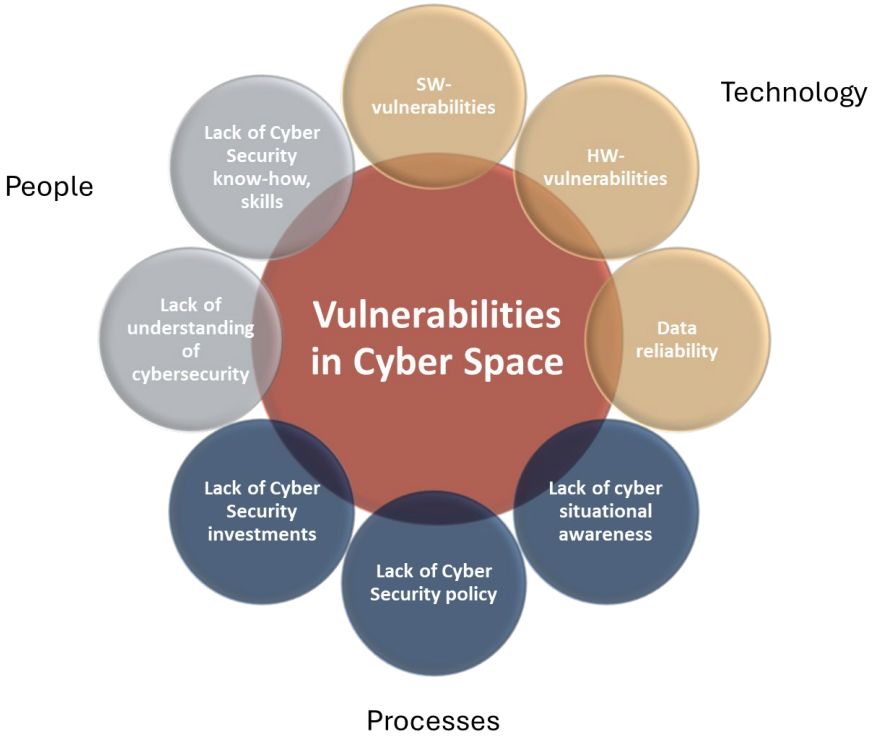

Figure 2: Vulnerabilities associated with cyber space of critical infrastructure

5.1 Vulnerabilities in People

People-related threats are referred to as insiders. These are people who have, or had, authorized access to information systems or information about an organization's information resources. Insider threats can be malicious and unintentional based on their intentions. A malicious insider may exploit their own access to information systems. Motives can include revenge, money, the need for recognition, or other personal reasons. An unintentional insider threat includes cases where an insider causes damage either through their actions or by failing to act. The most significant threat is unwary employees who fall for social engineering tactics like scam emails or phone calls. Social engineering is used by threat actors to take advantage of individuals' vulnerabilities by manipulating people through human interaction to form trust and confidence to compromise sensitive information. It is usually a matter of lack of knowledge and awareness that makes individuals most prone to phishing attacks. One group is made up of employees whose information system has been hacked due to the organization's poor cyber security. In this case, their computer is used to gain access to the organization's information system without their knowledge. (Ihanus, 2023)

Zimmermann and Renaud (2019) reported following vulnerabilities related to people at the individual level: 1) lack of cyber awareness, knowledge and skills, 2) lack of accountability, 3) lack of policies and compliance, 4) not following the best security practice, 5) not sharing responsibility, 6) malicious employees, and 7) cyber criminals (outside the organizations). The lack of cyber security awareness and knowledge may make individuals more prone to social engineering attempts, like phishing, as well as openly sharing information relevant to cyber security. The general issues with noncompliance with cyber security policies are known to be utilized for gaining access (Pham et al., 2017; Victor-Mgbachi, 2024). This connects vulnerabilities in cyber security policies with lack of proper security updates, inappropriate applications installed on critical systems, authentication weaknesses, unauthenticated PLC and remote terminal units (RTU) network connections, remote access supervision and interconnection management (ENISA, 2016).

5.2 Vulnerabilities in Processes

Vulnerabilities in processes include: 1) lack of cyber security know-how and skills, 2) lack of understanding of cyber security, 3) insufficient of cyber security investments, 4) lack of cyber security policy and 5) lack of cyber situational awareness.

The study in the United States identified the following process-related vulnerabilities for subsea telecommunication cables: 1) the private ownership of the cables and cross multiple jurisdictions, 2) the federal

review and permitting process for marine infrastructure may not consider cable protection; 3) lack of a robust protection strategy, 4) lack of a responsible federal agency on cable protection, and 5) gaps in leadership for reporting and investigating unusual activity, and facilitating cable issue resolution (Gallagher & Carter, 2023).

5.3 Vulnerabilities in Technology

Software vulnerability is a bug in program coding, configuration, or management. A program can be an algorithm, application, operating system or browser and control software like communication protocols and drives devices. Hackers exploit vulnerabilities in software attacks to force systems to give them access to unauthorized data, execute malicious code, obtain remote control, or cause the system to spread infections. The CyLab Sustainable Computing Consortium at Carnegie Mellon University estimates that "commercial software has 20-30 code bugs for every 1000 lines of code". Already over two decades ago, Applied Visions, Inc. estimated that 111 billion lines of new software code containing billions of vulnerabilities are coded every year. (Delio, 2004)

Hardware vulnerability is an exploitable weakness in a computer system that enables attack through remote or physical access to system hardware. Hardware vulnerabilities are difficult to identify. In January 2018, the entire computer industry was put on alert by two new processor vulnerabilities dubbed Meltdown and Spectre that defeated the fundamental OS security boundaries separating kernel and user space memory. The flaws stemmed from a performance feature of modern CPUs known as speculative execution. (Constantin, 2021)

IT/OT convergence (sub-aspect of sc. Industry 4.0) is the recent trend of increased connectivity between IT and OT systems, for various economical, strategical and operational reasons. However, this also introduces challenges to cyber security via widening of the attack surface. (ENISA, 2019; NSTAC, 2022)

5.4 SCADA-specific Issues

Nelligere et al. (2023) lists vulnerabilities among different levels, from process control to enterprise. Alanazi, Mahmood & Chowdhury (2023) divides the vulnerabilities into two categories: issues resulting from implementation and issues resulting from configuration. Upadhyay & Sampalli (2020) have these two analogous categories along with network security and protocol vulnerabilities.

Implementation

Improper validation of received input can lead to unintended privileges or otherwise unintended actions. Techniques might involve e.g. command or SQL injection, path traversal, or buffer overflow. Other failures to manage memory buffers can also result in further access or destruction of data. Control flow issues such as race conditions can also cause similar effects. (Upadhyay & Sampalli, 2020, Alanazi, Mahmood & Chowdhury, 2023)

Many of these issues are exacerbated by reliance on legacy protocols and devices, remote installations (this particularly applies subsea) and lack of knowledgeable people about particular of said systems. (Nazir, Patel & Patel, 2017, Nelligere et al., 2023)

Network and protocols

General principles of cyber security to great extent apply. Lack or improper configuration of firewalls/IDS/SIEM, network segmentation, access control lists and encryption are common issues. (Nelligere et al., 2023)

Proper encryption is not always feasible due to proprietary or legacy protocols involved, for e.g. MODBUS. In general, traffic sniffing, IP spoofing and Man-in-the-Middle attacks are among relevant vulnerabilities. (Upadhyay & Sampalli, 2020, Alanazi, Mahmood & Chowdhury, 2023)

Configuration

Weak password requirements, hard-coded credentials or other default passwords can enable the attacker to initially access or move around within the system. Also lack of encryption as mentioned previously can lead to exposed credentials. (Upadhyay & Sampalli 2020, Nelligere et al. 2023)

Deficiencies and faults in access control and authentication can also lead to undesired access to target network. Examples include (but are not limited to) bypassing authentication altogether, replay attacks and brute force attacks. (Alanazi, Mahmood & Chowdhury, 2023)

6. Impact Analysis

Impacts are the end point impacts that manifest after successful attack paths are completed, and they are agnostic to the techniques and technologies used. The effects of a cyber-attack can be diverse, such as: Account Access Removal, Damage to Property, Data Destruction, Data Encrypted, Data Manipulation, Web Page Defacement, Denial of System Control, Denial of Service, Disk Wipe, Firmware Corruption, Inhibit System Recovery, Loss of Availability, Loss of System Control, Loss of Productivity and Revenue, Manipulation of Control and View, Network Denial of Service, Resource Hijacking, Service Stop, System Shutdown/Reboot, Theft of Data and Information. (MITRE, 2025)

Impact propagation from affected systems to others is a risk in connected environment. Considering all the possibilities for attacks, it is resource intensive. Behind an attack there are varying triggers depending on the attacker archetype. One way to do an impact analysis is to create scenarios appropriate to the situation. Plausible scenarios can tell a story of what might happen. They give material for creating test cases and tabletop exercises, but do not comprehensively present everything that can happen. The more complicated scenarios aid in revealing dependencies between systems and events.

Cyber-attack models outline the structure of attack-vectors. Threat modelling abstracts a system, profiles potential attackers along with their goals and methods, and enumerates possible threats. By mapping potential attack paths and analyzing vulnerabilities through frameworks like MITRE ATT&CK, security analysts can understand attacker behavior, prioritize defenses, and reduce risk. (MITRE, 2025)

The study developed 14 scenarios for various cyber-attacks summarized in Table 2. The factors were initial access, vulnerabilities exploited, execution, attacker motivation, impact tactics, likelihood of attack and impact. The scenarios were ranked based on their individual estimated risks (impact x likelihood). (NIST, 2012) The overall risks of the scenarios presented are considered low or high. This overall risk represents a view that considers the target of the attack as well as the primary stakeholders. In this view, the highest risks were observed with scenario related to ransomware attack, and scenario related to exploitation of vendor-caused vulnerabilities. Considering the scenarios, we considered the top six most relevant scenarios, i.e. the ones that rank HIGH in risk. Out of these, we discerned the most utilized vulnerabilities. Table 3 illustrates most often occurring vulnerability categories and super categories in top 6 most relevant scenarios.

Table 2: Summary of developed scenarios

Scenario	Impact	Likelihood	Risk
Exploiting vendor vulnerabilities	HIGH	HIGH	HIGH
Malicious insider activities	MODERATE	HIGH	HIGH
Espionage on cable operators	HIGH	MODERATE	HIGH
Injecting false sensor information	MODERATE	HIGH	HIGH
Ransomware attack	HIGH	MODERATE	HIGH
Distributed denial-of-service attack	HIGH	MODERATE	HIGH
Phishing attack	MODERATE	MODERATE	MODERATE
Supply-chain attack	MODERATE	MODERATE	MODERATE
Hybrid attack (to energy network)	MODERATE	MODERATE	MODERATE
Private cable operator conducting espionage	HIGH	LOW	MODERATE
Misconfiguration of firewall	MODERATE	MODERATE	MODERATE
Credential exposure via misconfigured cloud	LOW	MODERATE	MODERATE
GPS spoofing	MODERATE	MODERATE	MODERATE
Fiber tapping telecommunication cable	LOW	LOW	LOW

Table 3: Most often occurring vulnerabilities

Vulnerability	Occurrences in scenarios
Lack of cyber security policy (super category)	6
Lack of understanding of cyber security (super category)	4

Vulnerability	Occurrences in scenarios
Poor cyber hygiene	4
Lack of security know-how and skills (super category)	3
General compliance issues	3
Lack of a robust protection strategy	3
Cyber security awareness is not a priority	2
Lack of preparedness for blackouts and internet outage	2
Dependencies on suppliers and service providers	2
Situational awareness not a priority	2
Insufficient cyber security investments	2
Low number of cable / pipeline access points / country	2
Insider threat	2
Operations divided and access granted to multiple operators	2
Lack of good practices in supply-chains	1
Lack of trained personnel	1
Private ownership of the cables	1

On a super category level, lack of cyber security policy was discovered to be a common factor in all the top 6 scenarios, with a closely related lack of understanding of Cyber security trailing closely behind with 4 scenarios, while rest of the super categories only concern 2 or 3 of the attacks. In addition, many of the most often occurring sub issues are contained within this, and thus formulation and upkeep of a quality cyber security policy is a natural recommendation for prioritization, if not in order already.

For example, one of the most significant initial attack vectors is phishing, thus having the personnel trained on the fundamental basics and up-to-date on the newest types of phishing attempts is crucial; this was singled out as one of the simple key issues in private discussions with a Digital Forensics and Incident Response (DFIR) operator. Training of personnel is key part of a cyber security policy.

Vendor-caused vulnerabilities scenario ranked HIGH both on likelihood and impact. Having a strategy in place for identifying and handling dependencies on suppliers and service providers is key in mitigating vendor-related vulnerabilities, both with respect to software and hardware, i.e. adopting a C-SCRM program (Cyber security Supply Chain Risk Management). This applies for both the external vendor-provided devices and software. According NIST Cyber security Framework 2.0: Quick-Start Guide for Cyber security Supply Chain Risk Management (C-SCRM) (NIST 2024; NIST, 2022):

- Having a Supply Chain Risk Management strategy (along with objectives, policies and processes) in place.
- List external technology suppliers and determine the criticality of each.
- Formulate relevant roles and requirements and communicate them to partners and stakeholders.

Where legacy systems cannot be updated or replaced, and as good practice in general, isolating the potentially vulnerable OT systems by network segmentation is crucial (as in the typical Purdue models). (Williams, 1992)

7. Discussion and Conclusion

Telecommunications and electricity sectors are considered critical and dependent on each other, hence possessing risks that an incident in one sector would affect the other (NIS Cooperation Group, 2024). All other sectors considered critical by European Union (2022a) are dependent on them. After identification of such vulnerabilities based on previous governmental, organizational and scientific reports, scenario-based modelling was conducted to consider various possible incidents that originate from cyber threats related to CSI. Based on the scenarios a rough risk assessment was made following common practices (NIST, 2012; ENISA, 2022). The risk assessment indicated that the overall risks caused by potential cyber threats are moderate to high with the greatest risks focused on the target organization. Cyber threats combined with vulnerabilities comprise cyber risks. In general, it is considered that cyber threats exist, and we cannot influence them, while we can reduce vulnerabilities to a point hence enabling us to manage the risks potentially to an acceptable level.

The study found that critical submarine infrastructure may be particularly vulnerable to cyberattacks due to organizational cybersecurity deficiencies. Potential key vulnerabilities include limited cybersecurity skills, lack of awareness, insufficient investment, fragmented policies, inadequate monitoring and shortcomings in technology. Additional concerns arise from private ownership and multinational supply chains. These conditions may complicate coordinated protection and risk management efforts across jurisdictions.

The research emphasizes the requirement for improved cyber security awareness, harmonized policy implementation, increased investment in training, and enhanced protection strategies, some of which have been recently implemented at the regulatory level in the EU but need to be brought to the organizational level.

It is expected that the resilience to cyber threats is increasing through investments and awareness training as well as the protective methods described above. This will help control the impact of the threat, as the likelihood of threats is on the rise. According to International Institute for Strategic Studies (Bentham, 2025), the vulnerabilities in telecommunication cables are increasing, as supposedly the attacks have become more feasible for smaller nations and others than state-sponsored actors. Hence, the mitigated risks are likely to remain balanced by the increase in likelihood and decrease in impact. In other words, the threat keeps rising, but we can perhaps reduce the vulnerabilities exploited.

Ensuring the integrity and resilience of subsea cable networks demands a blend of robust encryption, vigilant monitoring, international cooperation, cyber security policies and technical safeguards - measures essential to defending the digital world together.

Ethics declaration: An ethics declaration was not required for the research.
AI declaration: AI tools were not used in the creation of this paper.

References

Alanazi M., Mahmood A. and Chowdhury M. 2023. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues, Computers & security. https://doi.org/10.1016/j.cose.2022.103028

Bentham J. 2025. Subsea advances and challenges for the Asia-Pacific, retrieved 18.5.2025, https://www.iiss.org/online-analysis/online-analysis/2025/05/subsea-advances-and-challenges-for-the-asia-pacific/

Chesnoy J. 2016. Undersea Fiber Communication Systems. Academic Press.

Collins M. 2013. Analyzing Insider Threat Data in the MERIT Database, CERT Insider Threat Center, retrieved 15.1.2025. https://insights.sei.cmu.edu/insider-threat/2013/10/-analyzing-insider-threat-data-in-the-merit-database.html

Constantin L. 2021. 33 hardware and firmware vulnerabilities: A guide to the threats. retrieved 10.4.2025 https://www.csoonline.com/article/3410046/hardware-and-firmware-vulnerabilities-a-guide-to-the-threats.html

Delio M. 2004. Linux: Fewer Bugs Than Rivals, Wired blog, Dec 14, 2004, retrieved 25.9.2025. https://www.wired.com/2004/12/linux-fewer-bugs-than-rivals/

ENISA 2016. Communication network dependencies for ICS/SCADA Systems.

ENISA 2019. Industry 4.0 - Cybersecurity Challenges and Recommendations.

ENISA 2022. Interoperable EU Risk Management Framework.

ENISA 2024. ENISA Threat Landscape 2024.

Gallagher J. C. & Carter N. T. 2023. Protection of Undersea Telecommunication Cables: Issues for Congress. Congressional Research Service. R47648.

Hartikainen H. 2025. Technical cyber threats in undersea infrastructure, University of Jyväskylä, master's thesis.

Ihanus J. 2023. Sisäpiiriuhkan hyökkäysketju – sisäpiiriuhkan hyökkäysvaiheiden mallintaminen, University of Jyväskylä, Master Thesis.

Julkunen P. 2025. Cyber threat analysis of people and organizational processes in critical submarine infrastructure, University of Jyväskylä, master's thesis.

Lehto M. 2022. Cyber-attacks Against Critical Infrastructure, in Lehto M. and Neittaanmäki P. (Eds.) Cyber Security: Critical Infrastructure Protection, in series Computation Methods in Applied Sciences, Springer 2022, pages 3-42. ISBN: 978-3-030-91293-2.

Maasberg M., Zhang X., Ko M., Miller S. R., & Beebe N. L. 2020. An Analysis of Motive and Observable Behavioral Indicators Associated With Insider Cyber-Sabotage and Other Attacks. IEEE engineering management review, 48(2), 151-165. https://doi.org/10.1109/EMR.2020.2989108

MITRE 2025. MITRE ATT&CK ICS dataset. Accessed 5 May 2025, https://attack.mitre.org/resources/attack-data-and-tools/

Nazir S., Patel S., & Patel D. 2017. Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & security, 70, 436-454.

Nelligere S. L., Swamy G. T., Akheel M. A., & Chandramma R. 2023. Vulnerability Assessment and Analysis of SCADA and Foundation Fieldbus on Industrial Control System (ICS) Networks: A Literature Review. ICFAI journal of computer sciences, 17(2), 34-65.

NIS Cooperation Group 2024. EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors. European Commission.

NIST 2012. Special Publication 800-30 - Guide for Conducting Risk Assessments. U.S. Department of Commerce.

NIST 2022. Cybersecurity supply chain risk management practices for systems and organizations. U.S. Department of Commerce. NIST Special Publication 800-161r1

NIST 2024. NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM). NIST Special Publication No. 1305

NSTAC 2022. Information Technology and Operational Technology Convergence, President's National Security Telecommunications Advisory Committee.

ODNI 2017. Threats to Undersea Cable Communications. Office of the Director of National Intelligence.

Pham H.C., Brennan L. and Richardson J. 2017. Review of behavioural theories in security compliance and research challenges. Informing Science + IT Education Conferences, Ho Chi Minh City, Vietnam.

Reverdy D. & Skenderoski, I. 2015. Submarine Cables: Structuring and Financing Options.

UK-NCSC 2022. Reducing data exfiltration by malicious insiders, United Kingdom National Cyber Security Centre, https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders

Upadhyay D., & Sampalli S. 2020. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & security, 89, 101666.

Victor-Mgbachi T. 2024. Navigating Cybersecurity Beyond Compliance: Understanding Your Threat Landscape and Vulnerabilities. IRE Journals 7(7): 70-81.

Williams T. J. 1992. The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. Research Triangle Park, NC: Instrument Society of America.

Zimmermann V. & Renaud K. 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. International Journal of Human-Computer Studies 131: 169-187.