

SUBSEA CABLES - WHAT IS AT STAKE?

JULY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the EU's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu

CONTACT

For contacting the authors, please use resilience@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Georgia Bafoutsou, Maria Papaphilippou, Marnix Dekker, ENISA

ACKNOWLEDGMENTS

We would like to thank Mr Raynald Leconte, who was contracted by ENISA to support in the preparation of this report. We would also like to acknowledge the experts who contributed to this report by participating in interviews: Kent Bressie (Harris, Wiltshire & Grannis LLP, International Cable Protection Committee), John Wrottesley (ICPC Project Manager), Alain Polloni (Orange France), Tobias Liebetrau, Christian Bueger (SafeSeas and University of Copenhagen), Camino Kavanagh (King's College, London), Stasa Novak (NATO)

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2023

Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover:

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

Luxembourg: Publications Office of the European Union, 2023

ISBN: 978-92-9204-612-5, DOI:10.2824/212261 TP-08-22-342-EN-N



TABLE OF CONTENTS

1. INTRODUCTION	6
1.1 TARGET AUDIENCE	6
1.2 TARGET AUDIENCE	ERROR! BOOKMARK NOT DEFINED.
1.3 EU POLICY CONTEXT	6
1.4 METHODOLOGY	7
2. REGULATORY REGIMES, TREATIES AND PERMITS	8
2.1 NATIONAL REGULATORY REGIMES	8
2.2 INTERNATIONAL TREATIES	10
2.3 INSTALLATION AND REPAIR PERMITS	11
3. SUBSEA CABLE ECOSYSTEM	12
3.1 SUBSEA CABLE MAPS	12
3.2 SUBSEA CABLE ECOSYSTEM	12
4. CHALLENGES FOR SUBSEA CABLE RESILIENCE	16
4.1 ICPC STATISTICS FOR CABLE FAULTS	16
4.2 ROOT CAUSES FOR SUBSEA CABLE INCIDENTS	18
4.2.1 System failures	18
4.2.2 Human errors	18
4.2.3 Natural phenomena	18
4.2.4 Malicious actions	18
4.3 TECHNICAL CAUSES OF SUBSEA CABLE INCIDENTS	20
4.3.1 Power outages	20
4.3.2 Shunt faults	20
4.3.3 Cable breaks	21
4.3.4 Fibre failures	21



5. GOOD PRACTICES

22

6. CONCLUSIONS

24



EXECUTIVE SUMMARY

Subsea cables, are some of the most critical components of the global internet infrastructure. Estimates say that more than 97% of the world's internet traffic is transmitted via subsea cables. Subsea cables are therefore critical for the EU and protecting them from physical and cyber-attacks is strategically important.

Modern subsea cables use optical fibre technology to transmit communications data literally at the speed of light. Close to shore subsea cables are thicker and strengthened with armour, but for most of their length subsea cables have a diameter that is not much greater than that of a garden hose. While the number of subsea cables is growing constantly, in 2019 there were more than 378 subsea cables worldwide, spanning more than 1.2 million kilometres¹.

Subsea cables are covered by national telecom laws, but also by international treaties. In practice, a wide range of different authorities may be involved in the protection of subsea cables, including currently national competent authorities for telecom security, cybersecurity agencies, civil protection, defence, and coast guard.

Although subsea cables can be targets of malicious actions, for instance sabotage attacks, currently, the most common incidents affecting subsea cables have been accidental, unintentional incidents. Most often the unintentional cable damage is caused by commercial fishing and shipping activities. Sometimes, also natural phenomena can cause cable breaks, for instance underwater earthquakes. There are about 150-200 accidental, unintentional subsea cable faults every year².

The subsea cable landing stations, where the cable surfaces and connects to land-based infrastructure, are located on beaches or in cities, and they can be a weak point. Cable landing stations can be targeted by attackers, for example, with espionage attacks, deliberate power cuts, sabotage attacks with explosives, or even missile attacks in the case of a military conflict.

Repairing the damage to a subsea cable or to a subsea cable landing station is a complex and difficult, lengthy operation. Repair is also highly dependent on the availability of specialized and dedicated repair ships, of which there is only a limited number worldwide. In some areas repair may require powerful icebreakers, for instance. Given the complexity of repair operations and the scarcity of repair capacity, a coordinated attack against multiple subsea cables could have a major impact on global internet connectivity.

To mitigate the impact of potential incidents affecting the subsea cables and to ensure resilience of these interconnections, countries should take the following steps:

- Clarify the responsibilities and mandate of national authorities for the protection and security of subsea cables and the landing stations.
- Improve monitoring of subsea cables, across their entire length;
- Ensure that incidents affecting subsea cables and landing stations get detected and notified to all the relevant authorities;
- Ensure that subsea cable landing stations and the subsea cable network management systems are protected from physical and cybersecurity threats;

(1) <https://ccdcoe.org/uploads/2019/11/Subsea-cables-Final-NOV-2019.pdf>

(2) <https://www.csis.org/analysis/invisible-and-vital-subsea-cables-and-transatlantic-security>



- Promote diversification of subsea cable routes and diversification of cable types along the same route;
- Ensure that subsea cables are protected when they pass through shallow waters, for instance by burying them in the sea bed.

ENISA aims to follow up on this report with more detailed technical guidelines for national authorities, to support them with the technical aspects of the supervision of subsea cables and their associated infrastructure, including landing stations and cable network management systems.



1. INTRODUCTION

Subsea cables are some of the most critical components of the global internet infrastructure. This report gives a high-level overview of the global subsea cable ecosystem, the technical assets involved and concludes with some good practices for cable operators and governments.

1.1 TARGET AUDIENCE

This report is intended for national authorities in the EU who have a responsibility to supervise public communication networks and core internet infrastructure, under the European Electronic Communications Code³ (EECC) and the Directive on Security of Network and Information Systems (NIS2 Directive)⁴.

1.2 EU POLICY CONTEXT

European Electronic Communications Code (EECC)

Security requirements for operators of public communication networks and services are contained in Article 40 of the European Electronic Communications Code (EECC). EU Member States have transposed the EECC into national laws, and in each country, there are national authorities supervising the operators of public communication networks and services to ensure that they take appropriate security measures and report incidents with a significant impact.

Under the EECC (Art 40(3)), national authorities send summary reports about these significant incidents to ENISA and the European Commission, on an annual basis. In the past years national authorities have reported 12 subsea cable incidents to ENISA, all unintentional, accidental. However, because of their cross-border status, often spanning international waters, it is not always clear, who has the supervision mandate over subsea cables. Also, many subsea cable incidents do not reach the reporting threshold, because subsea cables are usually redundant, meaning that an incident with a single cable often does not cause a major outage.

Directive on Security of Network and Information Systems

The NIS2, the revision of the NIS directive, also covers the public communication networks and services, and it replaces the security requirements contained in Article 40 of the EECC. Subsea cables are explicitly mentioned in recital 97 of the NIS2:

(...) Since international connectivity enhances and accelerates the competitive digitalisation of the Union and its economy, incidents affecting subsea communications cables should be reported to the CSIRT or, where applicable, the competent authority. The national cybersecurity strategy should, where relevant, take into account the cybersecurity of subsea communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection.

Article 7 of the NIS2 asks MS to adopt policies, as part of their national cybersecurity strategies:

(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of subsea communications cables;

(3) <https://eur-lex.europa.eu/eli/dir/2018/1972/oj>

(4) <https://eur-lex.europa.eu/eli/dir/2022/2555j>

Note that both the EECC and the NIS2 Directive take an all-hazard approach, which means that they include cyber-attacks, but also physical attacks on network and information systems, including for instance unintentional damage of cables by shipping, or sabotage attacks. Physical attacks on critical infrastructure in general, is covered by the Critical Entities Directive (CER)⁵.

Nevers Joint call point 4

The informal Council meeting of Telecom Ministers, which took place in Nevers on 9 March 2022, resulted in a joint call to reinforce the EU's cybersecurity capabilities⁶. It recognised that *“critical infrastructure such as telecommunications networks and digital services are of utmost importance to many critical functions in our societies and are therefore a prime target for cyberattacks”*.

Point 4 of the call asks relevant national authorities, such as the Body of European Regulators for Electronic Communications (BEREC), the EU Agency for Cybersecurity (ENISA), and the NIS Cooperation Group (NIS CG) to make recommendations to EU Member States and the Commission, based on a risk assessment in order to reinforce the resilience of the EU's communications infrastructures and networks.

Subsea cables are in scope of the Nevers Joint call point 4 and are being addressed as part of this risk assessment.

1.3 METHODOLOGY

The methodology used for the creation of this report consisted of three parts:

- Desk research, taking stock of relevant literature on the topic
- Targeted interviews, with stakeholders in the area
- Consolidation and analysis of the information collected.

This report was validated by the experts who participated in interviews and by the members of the ENISA ECASEC group⁷, i.e. the national authorities responsible for telecom security in the EU.

(5) <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>

(6) <https://presse.economie.gouv.fr/download?id=92155&pn=2131> - Joint call to reinforce the EUs cybersecurity capabilities-
[pdf](#)

(7) <https://resilience.enisa.europa.eu/article-13>



2. REGULATORY REGIMES, TREATIES AND PERMITS

There is not a single regulatory regime for the protection of subsea cables. Several regulatory regimes, different national agencies, authorities and entities are involved.

At national level the lead entities are often the national telecom authorities⁸, who are supervising the security of the public communication networks and services. However, subsea cable protection and oversight also depends on other entities and agencies, for instance, surveillance by the coast guard, maritime law enforcement and police, or even marine rangers when cables are passing through marine protected areas.

In coastal zones and in territorial waters (up to 12 nautical miles) and within exclusive economic zones (EEZs), i.e. up to 200 nautical miles, subsea cables are protected by the navy, the military and the national coastguard. In international waters, and particularly outside the EEZs, the jurisdiction is more ambiguous and it is not clear which country is responsible for surveillance and protection of subsea cables.

At EU level there are several EU agencies with relevant mandate, including the European Union Agency for Cybersecurity (ENISA), the European Fisheries Control Agency⁹, the European Maritime Safety Agency¹⁰. Within the European Commission, several directorates-general are involved, including DG CONNECT (CNECT)¹¹, DG Mobility and Transport (MOVE)¹², or DG Maritime Affairs and Fisheries (MARE)¹³.

2.1 NATIONAL REGULATORY REGIMES

At national level, there are different regulatory regimes and different entities involved in protecting subsea cables and supervision.

In **France**, the Secretariat-General for National Defence and Security, an inter-ministerial organisation under the Prime Minister of France, plays an important role in ensuring and coordinating the national security perspective of subsea cable protection. The “Secrétariat général de la mer” coordinates all the administrative tasks relating to subsea cable protection.

In addition, the French Navy plays an important role in protecting cable installations in French waters in collaboration with private companies. Companies such as Orange Marine and Alcatel Subsea Network, which are world leaders in laying and maintaining subsea cables, perform themselves regular checks to detect and locate any faults.

(8) Chapter 6 of *Security Threats to Subsea Communications Cables and Infrastructure – Consequences for the EU* report of the European Parliament [https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA\(2022\)702557](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557)

(9) <https://www.efca.europa.eu/en>

(10) <https://www.emsa.europa.eu/>

(11) https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en

(12) https://transport.ec.europa.eu/index_en

(13) https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/maritime-affairs-and-fisheries_en

A range of other French public authorities also have mandates in subsea cable protection, such as the French National Cybersecurity Agency (ANSSI)¹⁴, the French Joint Defense Staff¹⁵, the Ministry for Europe and Foreign Affairs¹⁶ and the General Direction of External Security of the Ministry of Defense¹⁷.

In **Portugal**, several entities are responsible for the supervision of subsea cables, including the Autoridade Nacional de Comunicações - ANACOM¹⁸. The different entities involved coordinate between themselves.

ANACOM has developed protection measures to mitigate security risks to subsea cables and to facilitate their repairs. ANACOM focuses on three areas:

- An electronic portal for easy licensing (one-stop-shopping) for obtaining permits to install, maintain or repair subsea cables.
- An integrated environmental and seismic detection system using SMART Cables (wet detection),
- Investigation of several methods of dry detection (SoP, Phase Detection, DAS).
- A service for the protection and supervision of subsea cables, which is soon to be launched. A certified national public entity will produce warnings and alerts to ships near subsea cables routes within the Portuguese Exclusive Economic Zone. This will be a free public service, available 24 hours a day.

The Portuguese critical infrastructure law adopted in 2022 provides the legal framework for identifying, designating, protecting and increasing the resilience of critical infrastructure, consolidating in national law the transposition of Council Directive 2008/114/EC. The telecom sector is in scope of this legislation and although the classification of national critical infrastructures is currently ongoing, subsea cables could fall in scope of this classification.

In **Greece**, the Hellenic Authority for Communications Security and Privacy (ADAE)¹⁹ is the competent authority for security of networks and services of electronic communications providers. In that sense, monitoring effectiveness of security measures to minimize the risks and attacks on subsea cables, is part of ADAE's responsibility. ADAE is also the competent authority for auditing the providers for implementing the security measures concerning their preparedness in force majeure cases. However, second-level legislation which describes the detailed security measures for subsea cables has not yet been issued.

In **Bulgaria**, the subsea cable owners are responsible for cable security, while supervision is the responsibility of the Communication Regulation Commission (CRC).

In **Sweden**, the commercial entity that owns and operates the subsea cable is responsible for their security. Supervision and resilience initiatives are undertaken by the Swedish Post and Telecom Authority²⁰.

In **Slovenia**, the State Administration for Protection and Rescue²¹ is responsible for the supervision of subsea data cables.

(14) <https://www.ssi.gouv.fr/en/>

(15) <https://www.defense.gouv.fr/en/ema-s>

(16) <https://www.diplomatie.gouv.fr/en/>

(17) <https://www.dgse.gouv.fr/en/>

(18) ANACOM - Autoridade Nacional de Comunicações

(19) <http://www.adae.gr/en/>

(20) <https://pts.se/>

(21) About the Administration for Civil Protection and Disaster Relief | GOV.SI



2.2 INTERNATIONAL TREATIES

Cables are also protected under the following international treaties:

- **1884:** International Convention for the Protection of Subsea Cables^{22 23}.
- **1958:** Geneva Conventions of the Continental Shelf and High Seas²⁴.
- **1982:** United Nations Convention on Law of the Sea (UNCLOS)²⁵.

The international treaties establish universal norms:

- Freedom to lay, maintain and repair cables outside of a nation's 12 nautical mile territorial sea.
- National obligations to impose criminal and civil penalties for intentional or negligent injury to cables.
- Special status for ships laying and repairing cables.
- Indemnification for vessels that sacrifice anchors or fishing gear to avoid injury to cables.
- Obligations of cables crossing previously laid cables and pipelines to indemnify repair costs for crossing damage.
- Universal access to national courts to enforce treaty obligations.

UNCLOS, also referred to as the Montego Bay convention, defines legal boundaries in the ocean.

- **Territorial seas or territorial waters.** The zone of 12 nautical miles within which a country can limit activities related to subsea cables.
- **Exclusive Economic Zone (EEZ).** The zone of 200 nautical miles within which a country reserves the rights for some activities. UNCLOS considers that this EEZ is free for the installation of subsea cables, even if some countries require authorisation.
- **High Seas.** The rest of the seas, where there is free usage of the sea bottom for subsea cables.

(22) Convention for the Protection of Subsea Telegraph Cables - Wikipedia

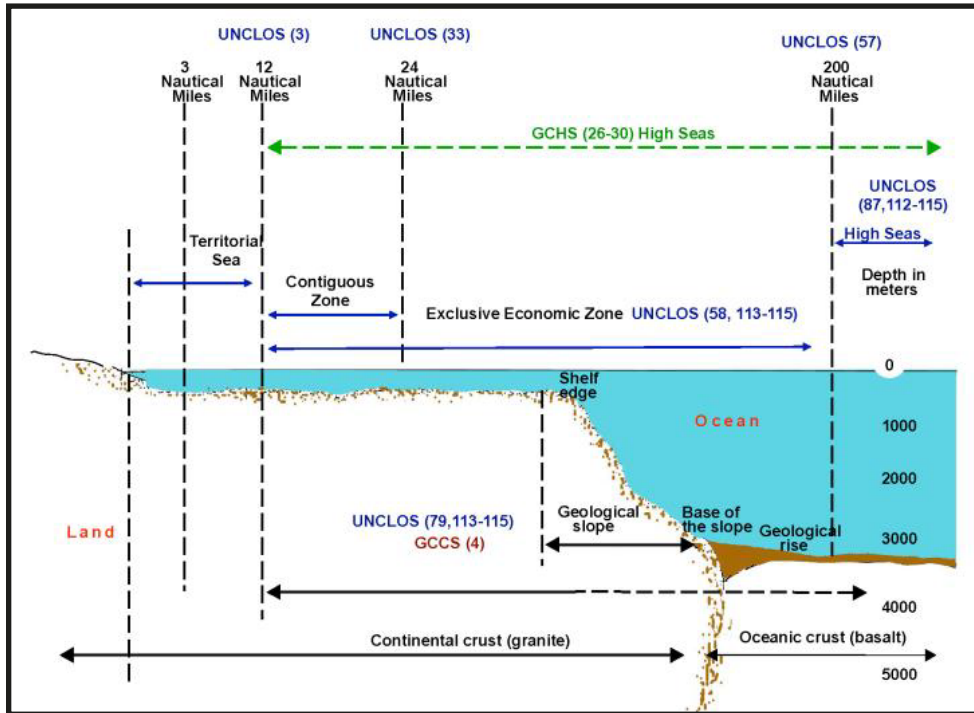
(23) <https://www.iscpc.org/documents/?id=13>

(24) <https://legal.un.org/avl/ha/gclos/gclos.html>

(25) https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf



Figure 1: Legal boundaries of the ocean (source: UNCLOS)



2.3 INSTALLATION AND REPAIR PERMITS

The process of “permitting” is a key issue for the installation of subsea cables. The installation of subsea cables in territorial waters requires ‘permits in principle’ issued by the national authorities. The permit process and format differ from one country to another.

Another key issue is ‘work permits’, which are required for vessels to operate in territorial waters for installation or repair of subsea cables. These permits can take some time to obtain and there is no defined international procedure.

Some countries have also adopted a ‘cabotage law’, under which only locally flagged vessels can work in territorial waters.

There are also cases where, even if this is not a provision of UNCLOS, permits are requested for installation or repairs within the contiguous zone (24 nautical miles) or within the EEZ (200 nautical miles), which may hamper installation of subsea cables when crossing these zones. This is the case, for example, for cables between Cuba and Guyana, which cross the EEZ of Venezuela, a country with strict relevant processes.

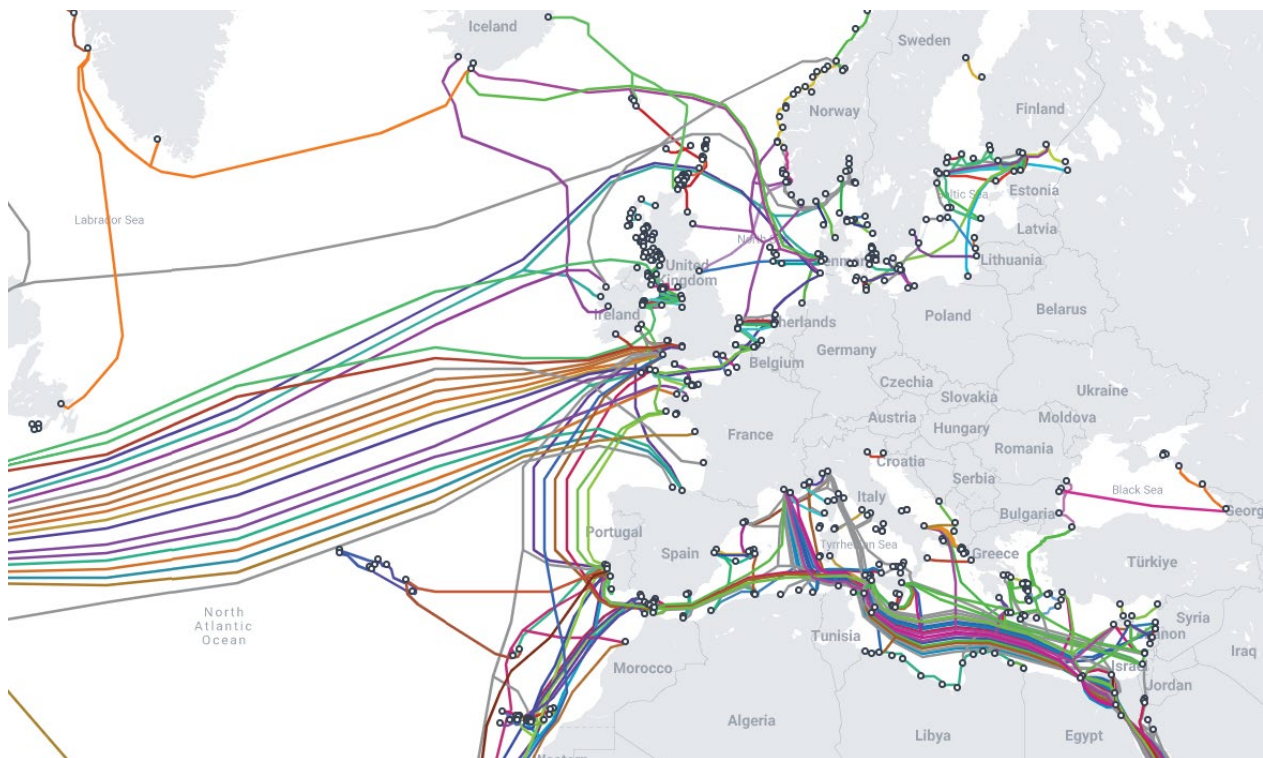
3. SUBSEA CABLE ECOSYSTEM

3.1 SUBSEA CABLE MAPS

One of the most comprehensive maps showing the overall global subsea cable infrastructure is the “Subsea Cable Map”²⁶. The Subsea Cable Map shows information per cable, its length, landing points and the owners of the cable. The cable maps can be filtered by cable system, country connected by cables, cable landing locations, suppliers.

The Subsea Cable Map is kept updated with data from TeleGeography²⁷, a telecommunications market research and consulting firm.

Figure 2: Subsea cable map (source: SubseaCableMap.org)



3.2 SUBSEA CABLE ECOSYSTEM

In the subsea cable ecosystem we distinguish the following stakeholders:

A. Owners and operators of subsea cables

(26) <https://www.subseacablemap.com/>
(27) <https://www2.telegeography.com/>

This category includes telecom operators like Orange²⁸, Telefonica²⁹, Telecom Italia Sparkle³⁰ and also private investors like EXA³¹, Aquacomms³², Lumen³³, Globenet³⁴ and Google, Amazon, Microsoft and Facebook, widely known as GAFAM.

B. Integrated suppliers

This category includes companies which manufacture and install subsea fiber optic cable networks, and also own and operate installation and maintenance vessels: Subcom³⁵, Alcatel subsea networks³⁶.

C. Suppliers without a fleet

Companies under this category produce cables and/or related hardware parts, and/or dry plant products such as power feeding equipment, Network Management Systems, but are not involved in the installation and maintenance processes: NEC³⁷, Xtera³⁸, HMN technologies³⁹.

D. Installation and repair vessel owners

This category includes companies that own and operate vessels for installation and maintenance of subsea cables: Subcom⁴⁰, Alcatel subsea networks⁴¹, Global Marine⁴², Orange Marine & Elettra⁴³, e-marine⁴⁴, Asean tableship⁴⁵, OMS group⁴⁶, Limin marine & offshore⁴⁷, SBSS⁴⁸, KT subsea⁴⁹, KCS⁵⁰, NTT We Marine⁵¹, International Telecom⁵².

In total, the above companies own around 35 vessels for cable installation and around 30 for cable maintenance⁵³.

E. Subsea cable maintenance

There are 2 types of maintenance agreements: agreements based on geographical zones (CMA) and private maintenance agreements on an ad-hoc basis. See the two maps below.

In the first case, the cable owners organise themselves to sign a **cable maintenance agreement** (CMA) based on geographical zones. The geographic zone agreements are as follows:

- Atlantic Cable Maintenance Agreement,

(28) <https://www.ecofinagency.com/telecom/1804-44436-orange-announces-new-subsea-cable-connecting-france-and-tunisia>

(29) <https://www.telefonica.com/en/about-us/countries-emerging-business-units/telefonica-infra/>

(30) <http://www.tiisparkle.com/our-assets/global-backbone>

(31) <https://exainfra.net/>

(32) <https://aquacomms.com/>

(33) <https://news.lumen.com/home>

(34) <https://www.globenetcorp.com/>

(35) <https://www.subcom.com>

(36) <https://web.asn.com>

(37) <https://www.nec.com/en/global/prod/nw/subsea>

(38) <https://www.xtera.com/>

(39) <https://www.hmntechnologies.com/>

(40) See Footnote 48

(41) See Footnote 49

(42) <https://globalmarine.co.uk/>

(43) <https://marine.orange.com/en/>

(44) <https://www.emarine.ae/>

(45) <https://www.aseancableship.com/>

(46) <https://www.oms.group/>

(47) <http://www.liminmarine.com/>

(48) <https://www.sbss.com/>

(49) <https://www.ktsubsea.co.kr/kor/Main>

(50) <https://www.k-kcs.co.jp/english/>

(51) <https://www.nttwem.co.jp/english/>

(52) <https://www.ittelecom.com/en/>

(53) <https://www.iscpc.org/information/cableships-of-the-world>

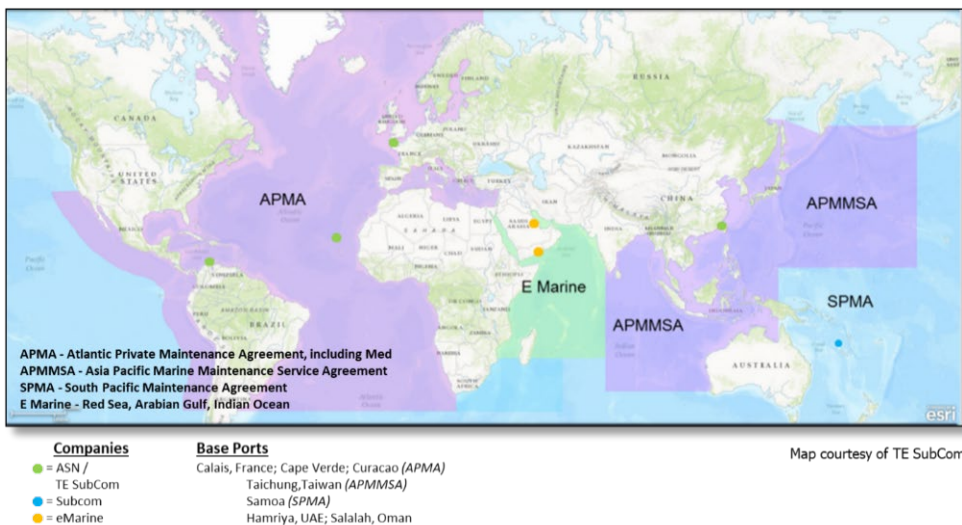
- Mediterranean Cable Maintenance Agreement
- Two Oceans Cable Maintenance Agreement
- South East Asia Indian Ocean Cable Maintenance Agreement
- Pacific Cable Maintenance Agreement divided into several regional zones (Yokohama, North America, etc.).

In the case of **private maintenance agreements**, the owners of maintenance ships propose a maintenance service for individual cables. Contracts are signed cable per cable. The priority of intervention in case of multiple cable faults is defined in each contract. The service provider also provides depot facilities. There is a notion of a base port, but the service provider can use its vessels for other activities. If the vessel is involved in other operations, mobilisation is not immediate.

Figure 3: Geographic cable maintenance zones (source: GMSL)



Figure 4: Private cable maintenance agreements (source: TE SubCom)





4. CHALLENGES FOR SUBSEA CABLE RESILIENCE

There are several challenges for the resilience of subsea cables. First, we look at the most comprehensive data set about subsea cable incidents, which is the list of cable faults and repairs maintained by ICPC, the International Cable Protection Committee. Then, we analyse the data about past cable incidents, by looking at root cause categories.

4.1 ICPC STATISTICS FOR CABLE FAULTS

The International Cable Protection Committee (ICPC)⁵⁴ was founded in 1958 and its membership comprises of governmental administrations and commercial companies that own or operate subsea telecommunications or power cables, as well as other companies that have an interest in the subsea cable industry – including most of the world’s major cable system owners and cable ship operators.

The primary purpose of the ICPC is to help its members improve the security of subsea cables by providing a forum in which relevant technical, legal and environmental information can be exchanged. The ICPC aims to promote awareness of subsea cables as critical infrastructure to governments and other users of the seabed. The ICPC has issued specific recommendations for states⁵⁵ and operators of subsea cables.

The ICPC report issued on 27 April 2022⁵⁶, includes data on cable repairs and cable faults. Based on this report, 185 repairs were conducted in 2021 within 44 different coastal jurisdictions.

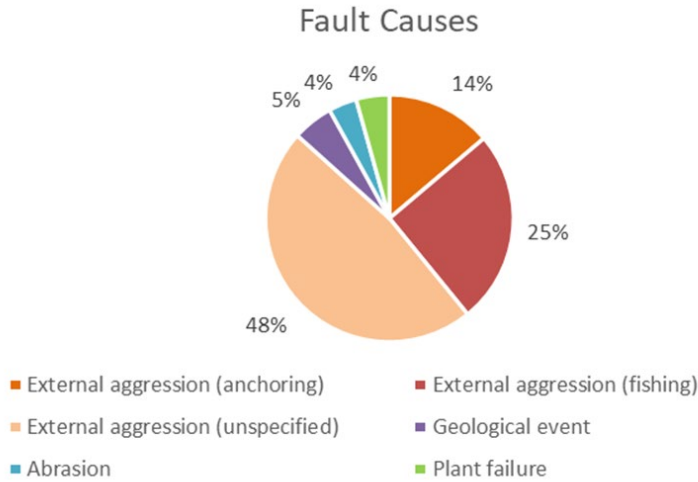
The 2022 report of the ICPC includes two graphs regarding cable faults and their type (electrical–optical):

(54) <https://www.iscpc.org/>

(55) Green, M., Drew, S., Carter, L. and Burnett, D., ICPC, ‘Subsea cable network security’, Subsea Cable Protection, Information Sharing Workshop, Singapore, 13 April 2009.

⁵⁶ *A Global Comparison of Repair Commencement Times: Update on the analysis of cable repair data*

Figure 5: Categorisation of cable faults (source ICPC report 2022)



From Figure 5, one can conclude that almost 40% of cable faults are due to anchoring or fishing, whereas for almost half of them the cause is unspecified. In total, 87% of incidents are caused by human intervention, either unintentional errors or intentional malicious actions. Only 4 % of incidents are attributed to system failures (plant failures) and 5 % are due to natural phenomena.

Figure 6: Fault types (source ICPC report 2022)

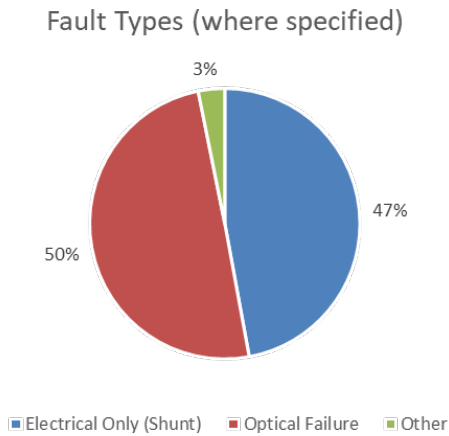


Figure 6, from the same report, shows that cable faults are evenly split between faults of the electrical system (shunt failures) and the optical system (fibre failures).

Over the years, ICPC has collected information about 2464 cable faults and repairs, covering 126 coastal jurisdictions, using data from 12 cable maintenance agreements⁵⁷.

- Atlantic Cable Maintenance Agreement, Mediterranean Cable Maintenance Agreement, North America Zone, Sentinel (IT Telecom Atlantic Private Agreement) and Yokohama Zone: 14 years of data from each.
- Telia ad hoc maintenance provision for the Baltic: 13 years of data.
- South East Asia and Indian Ocean Cable Maintenance Agreement, E-Marine Middle East Private Maintenance Agreement, TE Subcom/Alcatel private Maintenance Agreements, Atlantic Private Maintenance Agreement, Asia Pacific Private Maintenance Agreement and South Pacific Private Maintenance Agreement: 12 years of data from each.
- Two Oceans Cable Maintenance Agreement covering the South Atlantic and Indian Oceans: 9 years of data.

4.2 ROOT CAUSES FOR SUBSEA CABLE INCIDENTS

Below we analyse 4 broad root cause categories used by national authorities for telecom security incident reporting.

4.2.1 System failures

System failures, where a subsea cable breaks on its own, are not very common, because cables, cable repeaters and branching units are constructed based on standards with an extremely high reliability, usually defined as 23 failures in the 25-year lifespan of a system. System failures tend to be few in number. The ICPC report issued on 27 April 2022 (see Figure 5) shows that only around 4% of total failures are system failures, and they have been reducing in number.

4.2.2 Human errors

Human errors are a very common root cause for incidents with subsea cables. As mentioned above, most cable cuts and breaks are caused by marine activities. Fishing and anchoring are the most frequent cause of cable incidents (see Figure 5). Typically fishing activities affect a single cable, whereas anchoring may damage several cables at once, depending on the location.

4.2.3 Natural phenomena

Natural phenomena account for about 5% of cable incidents⁵⁸. They include seismic activity, mudslides, volcano eruptions, tsunamis and underwater currents during storms. Cable routes should be designed to avoid known zones of instability, but this is often impossible.

4.2.4 Malicious actions

There is not a lot of data about subsea cable incidents caused by malicious actions. There are many cable cuts in the ICPC data, for which the root cause is not known. There are not many confirmed reports in the media about malicious actions. There are several scenarios which should be taken into account:

1. **Sabotage attacks on subsea cables with the aim of disrupting connectivity**
Intentional, physical destruction of cables can be done with improvised cutting devices such as anchors and dredging devices, using subsea explosives, or with a submersible vehicle, either remote or subsea operated. Information on the cable routes can be easily be obtained and potential attackers can use other resources to obtain precise maps of the

(57) See Annex A for the definition of the maintenance agreements and maintenance zones.

(58) ICPC report issued on 27 April 2022, A Global Comparison of Repair Commencement Times: Update on the analysis of cable repair data.

sea floor. The duration and impact of such attacks is highly dependent on the distance from a spare cable storage and the availability of a cable repair ship. Lack of a pre-existing coordination mechanisms between countries and cable owners will also increase the time to repair.

The best way of preventing such attacks is through monitoring of civil maritime activities and the identification of anomalous behaviour. Preventing the use of explosives requires a combination of surface and subsea surveillance. Subsea attacks are difficult to detect and would require sophisticated underwater surveillance infrastructure along the entire length of the cable.

2. Espionage attacks on subsea cable to eavesdrop on communications data

Tapping of subsea cables at the seabed can be considered highly unlikely⁵⁹.

The reasons that support the above statement can be summed up to the following:

- For accessing the data passing through the cable, on the seabed, or at a subsea cable repeater, the optical fibres would have to be cut, which would generate alarms
- A dry environment would be needed to insert a tapping device. The signal in modern subsea cable systems uses coherent detection, with a local oscillator at a determined frequency, mixed with the signal of the line. This means that to access the data carried by the cable, there is a need to insert a local oscillator at the right frequency.
- The acquired information would need to be stored or transmitted. Transmission would require another large cable, because the volume of this information is several terabytes.
- The tapping device would also have to be powered, without disturbing the nominal power feeding of the system.

Eavesdropping on communications data through the cable network management systems or tapping of cables at the landing points is more feasible (see point 3).

3. Attacks against landing stations and network management systems

Every subsea cable has at least two landing stations where the subsea cable connects to the land. Landing stations are weak points and relatively vulnerable to physical and cyber security attacks.

Scenarios involving attacks to landing stations range from cutting power supplies to the detonation of improvised explosive devices, or even missile attacks. Landing stations are usually equipped with battery groups and power generator groups that operate in case of power supply failure from the public grid (normally with two independent points of access). However, such battery and generator sets can only ensure power supply for a few hours, not entire days, unless a continuous supply of fuel is ensured. Generator groups are also vulnerable to attack. Attacks on landing stations are likely to cause significant damage and can be difficult to repair quickly.

Historically, the operating centres located at or near these landing points, have largely been managed by on-site personnel or through tools that are not directly connected to the internet. Recently, however, more companies that manage subsea cable systems have connected their landing points and operating centres to remotely controllable network

(59) Morcos, P. and Wall, C., 'Invisible and Vital: Subsea cables and transatlantic security', Center for Strategic and International Studies, 11 June 2021.

management systems. By introducing a software-driven, 'virtualised' layer of control over cable systems – one connected to the internet – cable owners are exposing themselves to potential hacks of subsea cables through that technology. Obtaining illegal access to network management systems of cables can give visibility of networks and data flows, knowledge of physical cable vulnerabilities and the ability to monitor, disrupt and divert traffic⁶⁰. Finally, using of legacy IT or proprietary solutions, with security vulnerabilities which are not regularly patched, can be an additional security concern.

4. Attacks on repair vessels

Malicious actions against repair vessels should also be considered. Only two cable ships are based in the European Union, with an additional one based in the United Kingdom. Ships and depots are vulnerable to the entire spectrum of weapons used on land (e.g. improvised explosive devices, missiles) and against marine vessels (marine improvised explosive devices (MIEDs), torpedoes, missiles).

Given the importance of the repair infrastructure, a coordinated attack involving sabotage of cables and attacks on repair ships could cause long-lasting outages.

4.3 TECHNICAL CAUSES OF SUBSEA CABLE INCIDENTS

The most common technical causes of subsea cable incidents are power-cuts, shunt faults, cable breaks, and fibre failures.

4.3.1 Power outages

Fibre-optic data cables longer than 150 km require electric power to function, because repeaters need to compensate for signal losses over distance⁶¹. As a rule, electricity can be supplied from both cable landing stations, making a data cable power outage scenario less probable. However, power outages which affect both cable landing stations can result in a loss of connectivity.

4.3.2 Shunt faults

Shunt faults are the most common subsea cable faults. In this type of failure, the cable structure is damaged, either by trawl, anchor or abrasion/chafing. The power feeding structure is exposed to the sea and becomes a sea earth to the power feeding path. Damage to the fibres within the cable may also occur.

In this type of failure, since it is normally possible to continue to power the cable, at least from one end, the power feeding equipment (see Annex B for a description of a subsea cable system) can find the voltage drop to the fault and therefore calculate the cable distance to the fault.

Direct Current (DC) resistance measurements on the unpowered cable are also performed to the fault, in order to confirm this distance. An electroding tone can be applied to the cable by modulating the power feeding equipment line current at a frequency of 25 Hertz. By deploying simple tone-detecting sensors, the cable ship is assisted in locating the cable, which has often been pulled away from its laid position by the source of external aggression. If the fibres are broken in the first repeater section, optical time domain reflectometer equipment (OTDR)⁶² can be used to measure the fibre continuity to the fibre break. The distance can then be read directly from the instrument, which converts time to distance using the looped velocity value.

(60) Public-Private Analytic Exchange Program (AEP), 'Threats to Subsea Cable Communications', Department of Homeland Security, 28 September 2017.

(61) Agrawal, G. P., 'Optical Communication: Its history and recent progress', Optics in Our Time, 2016, pp. 177–199.

(62) A device that analyses the reflexion of a signal at the broken end of a fibre.

The subsea cable protection and supervision service to be implemented in Portugal as mentioned previously in section 2.1, involves integrating detection through SMART Cables and other methods of detection without recourse to the use of wet sensors, but also, among others, a vessel warning and the production of incident occurrence reports.

4.3.3 Cable breaks

Cable breaks occur when the cable is completely broken. To break a cable, especially one which is armoured, requires considerable tension.

In such faults, provided power can still be applied, a similar range of tests can be used as previously outlined for shunt faults.

Cable breaks are more often attributed to anchor damage, but heavy fishing equipment pulled by powerful trawlers may also be responsible.

4.3.4 Fibre failures

A fibre failure takes place when a fibre breaks within an intact cable structure or at some distance from the cable fault. This failure may result from excessive residual strain on the fibre. This may be caused by excessive tension being applied to the cable, or more likely because the maximum bending diameter of the cable has been exceeded.

This may be the result of loops or kinks being formed on the seabed during the laying or recovery of the cable. In this situation, OTDR⁶³ or Coherent OTDR (COTDR) equipment is used to locate the position of the fibre break.

(63) See Footnote 29

5. GOOD PRACTICES

In this section we list several good practices around subsea cable protection that should be taken into account by governments and cable operators.

Good practice	Who?	Why?
<i>Diversification</i>		
Cable diversity in the same route	Cable owners, cable operators	To avoid simultaneous damages in multiple cables in the same route
Geographic diversity of routes and landings of cables	Governments	To avoid single point of failure
<i>Cable installation, operation and maintenance</i>		
Identify the safest cable route and select the best cable type for each part of the route	Cable owners, cable operators	To avoid cable incidents due to commercial marine activities like fishing and anchorage
Bury cables into the seabed, especially for shallow water (depths of less than 1500 meters)		
Ensure spatial separation of subsea cables from marine activities	Governments	
Regularly update nautical maps and charts, including the location of subsea cables		
Designate subsea cable protection zones		
Establish annual pre-clearance procedures for cable ships and crews for repairs and maintenance in territorial waters		
Avoid defining subsea cable installation and repair as requiring cabotage. Avoid cabotage or crewing restrictions on vessels engaged in installation or repair of subsea cables, whether in territorial waters and EEZs.	Governments	To avoid delays in repairs and general maintenance activities
Establish a single point of contact for permitting, and any issues arising around cable installation, repair, and protection		
Use of automated identification and early warning systems for cable incidents	Cable operators	To avoid delays in incident detection and increased impact

Protect cable landing stations and the security of beach manholes	Cable operators	To avoid attacks on the land-based part of subsea cables
<i>Regulatory Regimes</i>		
Appoint a national lead agency	Governments	To avoid fragmentation of responsibility and confusion
Establish surface surveillance of civil maritime activities and enhance subsea surveillance		
Develop standard procedures for notification of incidents and other suspicious activities	National lead agency	To gain threat intelligence
Coordinate information sharing regarding vulnerabilities and threats		To enhance prevention mechanisms
Organize regional bilateral and multilateral and exercises		

6. CONCLUSIONS

Subsea cables are critically important for global internet connectivity. More than 97% of the internet traffic passes through subsea cables.

Although, the global internet interconnections and the subsea cable network is designed to be resilient and redundant, there have been several subsea cable incidents that have reached the media over the years and have caused outages or service disruption.

The most common incidents are caused by human errors, typically marine activities like fishing and anchoring.

A small percentage of incidents are caused by natural phenomena, such as underwater earthquakes, and general system failures, where the subsea cable breaks by itself. There is no good data on malicious actions affecting subsea cables, but relevant risk scenarios related to sabotage attacks on subsea cables and especially chokepoints should be considered. The subsea cable landing stations, where the cable surfaces and connects to land-based infrastructure, are located on beaches or in cities, and they can be a weak point. Cable landing stations can be targeted by attackers, for example, with espionage attacks, deliberate power cuts, sabotage attacks with explosives, or even missile attacks in the case of a military conflict.

Having single points of failure with concentration of cables in a single route or lack of diversity of routes, amplifies the risk of a coordinated attack on several cables and it would strain the repair capacity. Also, unintentional damage through fishing or anchoring or a natural phenomenon (subsea earth quake, subsea landslide) could affect many cables at once and thus compromise key routes.

At national level it is not always clear which authority should have the power to supervise subsea cables and receive incident reports concerning subsea cables. It is important that the EU Member States clarify at national level who has the responsibility and mandate for the protection and security of subsea cables.

It is also important that the relevant national authorities start exchanging good practices about the protection of subsea cables. This exchange of good practices should take into account good practices from the energy sector about protection and security of subsea power cables, as well as good practices from the authorities responsible for physical security of critical infrastructure under the Critical Entities Resilience Directive⁶⁴.

ENISA aims to follow up on this report with more detailed technical guidelines for national authorities, to support them with the technical aspects of the supervision of subsea cables and their associated infrastructure, including landing stations and cable network management systems.

Finally, it is important to better understand the redundancy and capacity of subsea cables and if there are single points of failures presenting high risks for international connectivity in the case

⁽⁶⁴⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829>



of a large incident. To analyse this better, the European Commission recently launched a dedicated project to analyse further the redundancy and resilience of subsea cables.



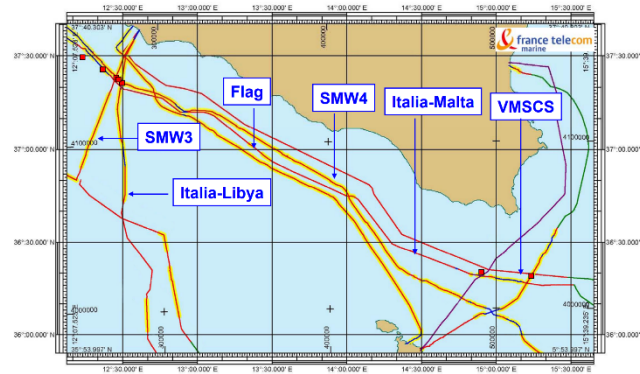
ANNEX A: SUBSEA CABLE CUTS

In this Annex we give an overview of cases, reported in the media in the past years, where subsea cables were cut or damaged.

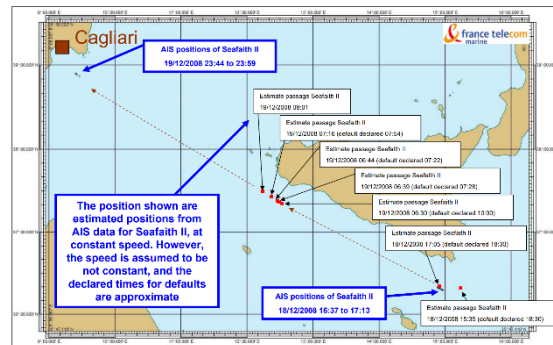
Note that particularly in 2008 there were a number of cable breaks involving subsea cables in the Mediterranean, connecting Europe and the Middle East.

23 January 2008	1 million internet users were affected by a cable cut of the FALCON subsea cable on 23 January. The FALCON cable system connects several countries in the Persian Gulf and India.
30 January 2008	<p>On 30 January 2008, news agencies reported that internet services were widely disrupted in the Middle East and the Indian subcontinent following damage to the SEA-ME-WE 4 and FLAG TELECOM cables in the Mediterranean Sea. The damage to the two systems occurred independently, several kilometres apart from each other, near Alexandria, Egypt. The cause of the damage to the cables was not revealed by either cable operator. A number of sources speculated that it was caused by a dragging ship anchor near Alexandria. The Economist reported that an earthquake may have been the cause.</p> <p>The effects on data traffic were measured from the end of December 2007 to the beginning of February 2008. Disruptions of 70% in Egypt and 60% in India were reported, along with problems in Afghanistan, Bahrain, Bangladesh, Kuwait, the Maldives, Pakistan, Qatar, Saudi Arabia and the United Arab Emirates. Around 1.7 million internet users in the United Arab Emirates were also affected by the disruption. Services were largely restored within 24 hours of the cable cut by diverting traffic through the TIC and SEA-ME-WE 3 cables.</p>
1 February 2008	Two days after the initial cable break of FALCON on January 23rd, it was reported that the FALCON cable was cut between Muscat (Oman) and Dubai (United Arab Emirates). This cut was between different landing points and was caused by an abandoned anchor weighing 5–6 tonnes.
3 February 2008	On 3 February 2008, a cable connecting Qatar to the United Arab Emirates had been damaged, causing disruptions in already damaged Middle Eastern communication networks. The problem was said to be related to the power system of the cable.
19 December 2008	<p>On 19 December 2008 it was reported that cables, linking Alexandria (Egypt), Sicily (Italy) and Malta, had been severed by either bad weather conditions or a ship's anchor, resulting in substantial slowdowns in communication traffic, with Egypt experiencing an overall 80 % reduction in internet capacity. The GO-1 cable connecting Sicily and Malta was also cut.</p> <p>The break disrupted 75 % of communication between the Middle East and Asia and the rest of the world.</p> <p>Rerouting of communications due to the damages caused large slowdowns in some areas.</p> <p>This event was so significant that the cable owners ordered an investigation for the causes of such a widespread damage. Based on the results of that investigation, a vessel anchor was found with a route crossing all the cables.</p>

The cuts were at 400 metres deep. Other cables at greater depths were not affected.



Map of subsea cables in Southern Sicily affected by the incident



Details

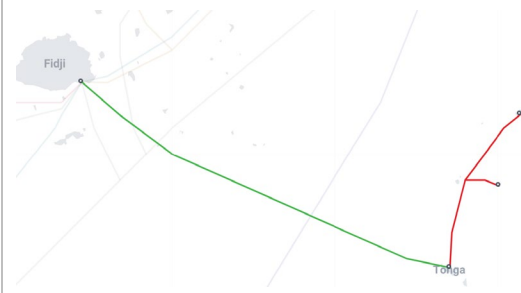
of the faults

A survey of the seabed found anchors scars in that area. The consequences were drastic for Maltese communications. The traffic between Asia–India and Europe slowed down for several days. The close proximity of the cable ship bases and the availability of spares were both factors that influenced the high speed of the repairs.

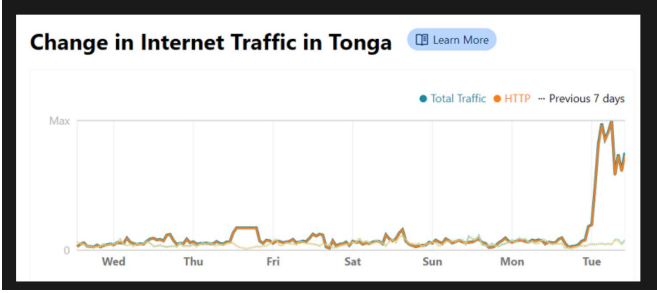
<p>25 December 2011</p>	<p>This disruption refers to two incidents of subsea communications cables cut off on 25 December 2011⁶⁵.</p> <p>The first cut-off occurred to SEA-ME-WE 3 in the Suez Canal (Egypt) and the second occurred to I2I between Chennai (India) and Singapore. These incidents caused internet disruptions and slowdowns for users in South Asia and the Middle East, particularly in the United Arab Emirates.</p>
<p>Japan 2011</p>	<p>Following the Tōhoku earthquake in 2011, four out of 20 subsea cables to Japan were ruptured⁶⁶. These simultaneous outages seriously impacted inter-Asian and transpacific internet traffic. In this case, the loss of bandwidth could be compensated for with Japan’s remaining cables.</p>

(65) https://en.wikipedia.org/wiki/2011_subsea_cable_disruption.

(66) W. Qiu, 'Subsea Cables Cut after Magnitude - 9.0 Earthquake and Tsunami in Japan', Subsea Cables Network, 12 March 2011

<p>Angola 2020</p>	<p>In January 2020, the South Atlantic 3/West Africa (SAT-3/WACS) cable, linking Africa to Portugal and Spain, was hit by a breakdown in Gabon, whilst the West Africa Cable System (WACS) that connects South Africa to the United Kingdom saw an outage off the coast of the Democratic Republic of the Congo. The fault on SAT-3 was caused by sand and mudslides.</p>
<p>Tonga 2022</p>	<p>Tonga is linked to the rest of the world by one cable, the Tonga cable between Nuku'alofa and Suva (Fiji). On 16 January 2022, an eruption of the Hunga Tonga-Hunga Ha'apai volcano sent tsunami waves across the Pacific Ocean, so that connectivity was lost on the line operated by Tonga Cable Ltd in waters about 37 kilometres (23 miles) offshore⁶⁷.</p>  <p>Map of subsea cables linking Tonga islands (2019)</p> <p>The Tonga cable and the Tonga Domestic Cable were damaged. The repair of Tonga's critical 827-km (514-mile) fibre-optic link to Fiji depended on the arrival of a specialised ship located days away in Port Moresby, the capital of Papua New Guinea.</p> <p>SubCom Reliance was mobilised and completed the necessary repairs to both cables within 8 days of arrival on the repair grounds. Tonga's international subsea cable was repaired, more than a month after it was damaged by the underwater volcanic eruption.</p> <p>The repairs took place under the South Pacific Marine Maintenance Agreement. Closer inspection of the damage revealed that there was more extensive damage, than originally considered. A new length of cable was laid to replace the damaged section.</p> <p>During the outage, Tonga relied only on satellite services. The Figure below shows the traffic before the repair. The low value is traffic on satellite only. The situation returned to normal only when the subsea cable was repaired.</p>

(67) <https://www.datacenterdynamics.com/en/news/tongas-international-subsea-cable-repaired-after-volcanic-eruption/>.

	 <p>Internet traffic Tonga subsea cable outage (source: Cloudflare)</p>
<p>Taiwan 2023</p>	<p>Two subsea cables connecting the Taiwan-controlled Matsu islands, which sit close to the Chinese coast, were cut, disconnecting from the internet the 14,000 people who live there⁶⁸. A backup microwave system that transmits signals from the top of a mountain in Taipei to Matsu was switched on, but that only restored about 5% of the bandwidth that the cables had provided. The island residents were informed that they had to wait until late April for internet access to be fully restored.</p>

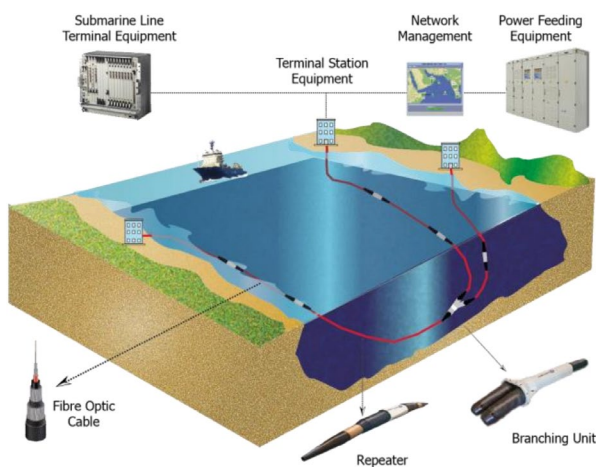
(70) <https://www.reuters.com/world/asia-pacific/fear-dark-taiwan-sees-wartime-frailty-communication-links-with-world-2023-03-15/>

ANNEX B: TECHNICALITIES OF SUBSEA CABLES

In this Annex we discuss some of the technical details of a subsea cable system.

Installation close to shore

Close to shore, a subsea cable⁶⁹ is buried with a plough on board the cable ship. The landing operation consist of pulling the cable from the cable ship to the beach manhole. The cable on the beach or in the water near the beach is buried and protected by metallic articulated protection.



Landing stations

Landing stations play a key part in the operation of subsea cables. They can perform many functions, including terminating international cables, supplying power to cables and acting as a point of domestic and/or international connection⁷⁰. In these landing stations, there are systems needed for the functioning of the cable network – such as heating, ventilation and air-conditioning systems. In the landing stations the following components are found:

- optical terminal equipment;
- multiplexing equipment to optimise the capacity of the cable;
- power feeding equipment;
- supervision equipment.

Today, landing stations are installed in containers in a normally well-known and easily accessible protected perimeter, whereas in the past they were installed in structured buildings and in some cases were very well protected (typical of the 1960s). Landing stations host servers and provide the bridge to the terrestrial network using routing and switching technologies. They tend to be physically protected by fences or barbed wire and remote surveillance equipment, such as cameras and sensors. The precise locations of landing stations are not in the public domain, although there are indicative maps that can potentially lead to their identification.

(69) Source: Alcatel Subsea Network.

(70) <https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-subsea-cable-security/>.

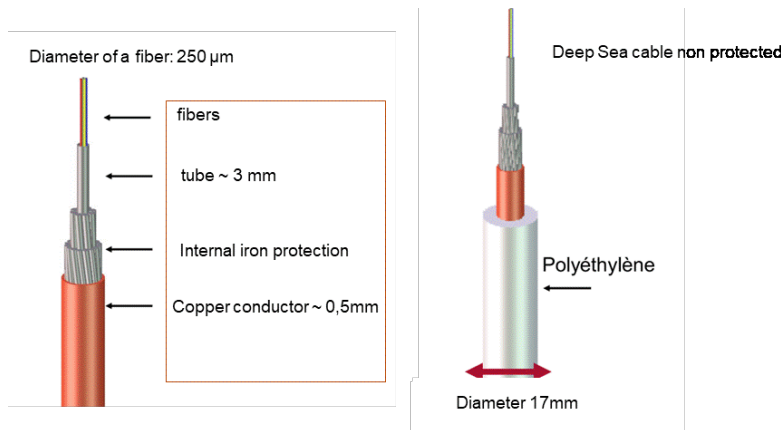
Since cables land in beaches that are easily accessible and the landing locations can be found, for instance, on the Telegeography Cable Map⁷¹, landing points of subsea cables in the “beach manhole” are vulnerable sites.

The supervision equipment measures the optical output of each fibre and the power inserted in the cable. The cable supervision system can detect any variation of the signal and a potential shunt fault affecting the power feeding. There is also supervision of every repeater and branching unit.

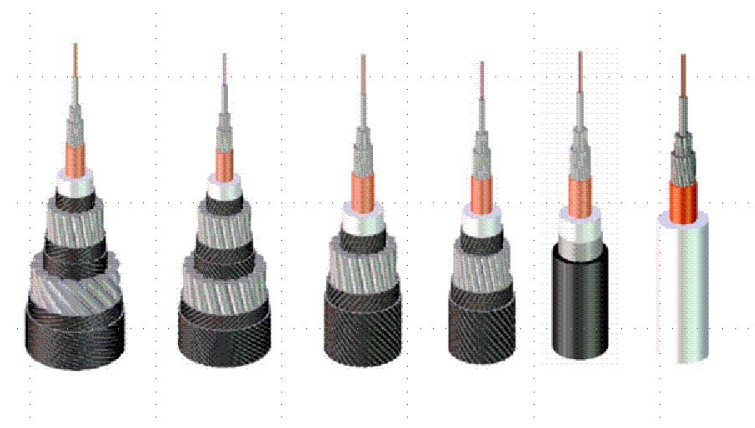
In case of fault, the supervisor can be used determine the position of the fault by OTDR. This emits a train of fast pulses and analyses the magnitude, duration and shape of the reflected pulses. The distance in the cable has to be translated in distance with the description of the route (straight line description). For electrical faults, Ohm’s law determines the position of the fault. The distance is also computed using the SLD.

Subsea cable structure

Subsea cables are quite thin (not much thicker than a garden hose). Depending on the location the cable has more or less armour. Large parts of the cable, where it passes through deep sea, are not armoured.



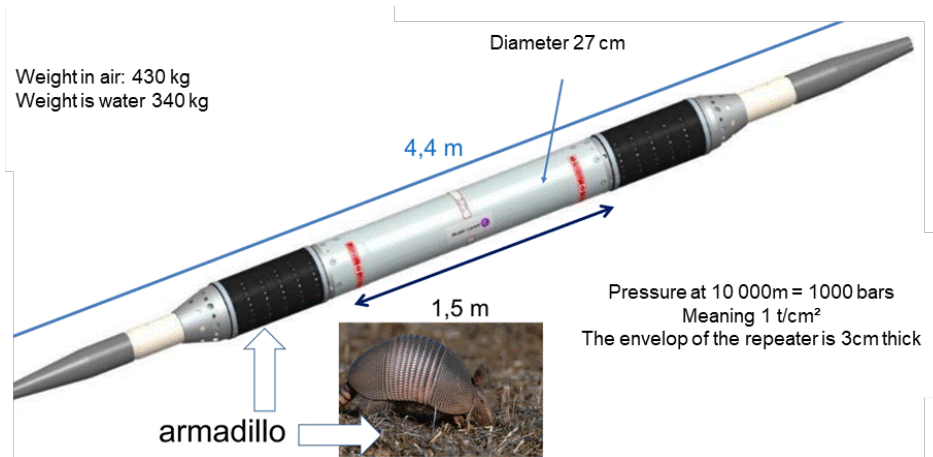
From right to left ⁷², from no armour (for the deep sea) to double armoured (for shallow waters).



(71) <https://www.subseacablemap.com/>.
 (72) Source: Alcatel Subsea Network.

Branching units

A branching unit is a piece of equipment that links three directions.



Cable element and network management system

Every component of a subsea cable system is supervised by an element management system (one FPE, one repeater, etc.) and by a network management system.

Among others, the following parameters are constantly monitored:

- fibre per fibre, the optical attenuation and other properties like polarisation;
- active equipment repeater and branching unit;
- power feeding.

Any event is immediately reported to the operating support system. The events are immediately reported to the network operation centre and to the different system user's network management systems.



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira

700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

