COMMITEE: ITU- Critical Digital Infrastructures
ISSUE: How can the international community strengthen the protection of submarine cables against hybrid threats and geopolitical tensions in order to ensure the security of global communications and safeguard States' sovereignty?
CHAIRS: John-Tyler Duperoy, Maya Yankovskaya, Mathilda Rey

PRESENTATION OF THE CHAIR



Hello, dear delegates!
My name is Mathilda Rey, I am 17 years old and I am a student in the german section of the international high school of Ferney-Voltaire. I love traveling, listening to music and discovering new sports. I have been doing gymnastics for a few years. For my last FerMUN conference, I will have the pleasure of chairing the Critical Digital Infrastructure Committee alongside John-Tyler and Maya. Our committee will address a very current issue concerning the protection of submarine cables. These cables are indeed essential for communication and intercontinental transactions, but are therefore targeted by sabotage and espionage attempts. We will seek to find solutions that ensure the security of global communications and preserve the sovereignty of states.

KEYWORDS

Critical digital infrastructure: All the infrastructures essential to the functioning of a state thanks to digital technologies (Internet, telecommunications networks, data centres, satellites, submarine cables, etc.).

International community: All states, international organizations, companies and other actors that cooperate at the global level.

Submarine cables: Optical fibers installed at the bottom of the oceans that transport data between continents. More than 95% of international data traffic (internet, phone calls, banking transactions, government communications) passes through these cables. They are therefore essential to the functioning of the global digital economy.

Hybrid threats: Actions combining several means (cyberattacks, sabotage, disinformation, economic pressure, espionage, indirect military actions) to destabilize or weaken a state without officially declaring war.

Sovereignty of States: The principle that each state is independent and exercises authority over its territory without external interference. In the digital domain, this means that a state must be able to protect its strategic infrastructure and guarantee control over its essential communications.

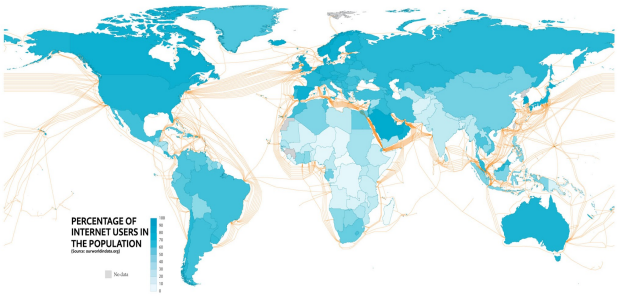
Cyberspace: Cyberspace is the global digital space formed by the interconnection of networks, information systems and telecommunication infrastructures.

OVERVIEW

To better understand the importance of submarine cables, we recommend watching the following video:
Thin underwater cables hold the internet. See a map of them all.

I. Submarine cables: a vital infrastructure

Submarine fiber-optic cables are an essential infrastructure for the global digital world. According to this review by François Lambert, they carry about 98% of international communications, including Internet exchanges, telephone calls and financial transactions. Diplomatic communications and some military communications also pass through these cables. Cyberspace depends heavily on this network of cables. The French National Agency for Information Security (ANSSI) also defines cyberspace as the communication space resulting from the global interconnection of digital equipment.[1]



The history of submarine cables dates back to the 19th century, with the first telegraph cable installed in 1851 between Calais and Dover. This facilitated exchanges between the financial centers of London and Paris. A few years later, in 1858, the first transatlantic cable connected Ireland to Newfoundland. Since then, technological advances have improved the performance of cables. Copper telegraph cables have gradually been replaced by fiber optic cables that can transmit large amounts of data at very high speed. Today, hundreds of submarine cables form a global network that connects all continents. The development of the Internet and globalization has increased the dependence of states on this infrastructure. Every day, billions of dollars in financial transactions pass through these cables.[2]

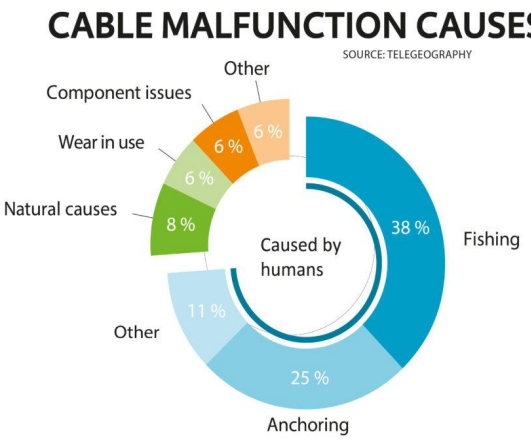
[1] https://millenniumprize.org/news-articles/news/supergraph-the-information-network-under-the-sea/

[2] news.un.org

II. Why are they vulnerable ?

Even a temporary interruption can have significant economic and political consequences. Despite their importance, underwater cables are vulnerable. They can be damaged by natural disasters or human activities. Among the accidental risks, we can observe the degradation coming from the anchors of ships and fishing boats. Off the coast, cables usually rest directly on the seabed and can be damaged by earthquakes or underwater landslides. The damage may also result from intentional actions, notably in the context of sabotage or espionage operations.

These physical vulnerabilities can be exploited in hybrid threats, where actors combine covert sabotage, cyber attacks and disinformation operations to destabilize a state without direct confrontation.[3]



Moreover, behind the image of an immaterial Internet "in the cloud" lies a highly strategic but also vulnerable physical network. A fragility that is now emerging as a major geopolitical issue.

Several of the world's most strategic submarine cable routes run through the Middle East. The narrow passages of the Red Sea, the Bab el-Mandeb Strait, the Suez Canal and the Strait of Hormuz have become true "digital chokepoints". The main problem with submarine cables is their concentration. Many use the same routes at the bottom of the sea and converge on a very limited number of strategic maritime crossings. This concentration creates major points of vulnerability. A cable outage, either intentional or accidental, can disrupt connections in multiple regions worldwide simultaneously.

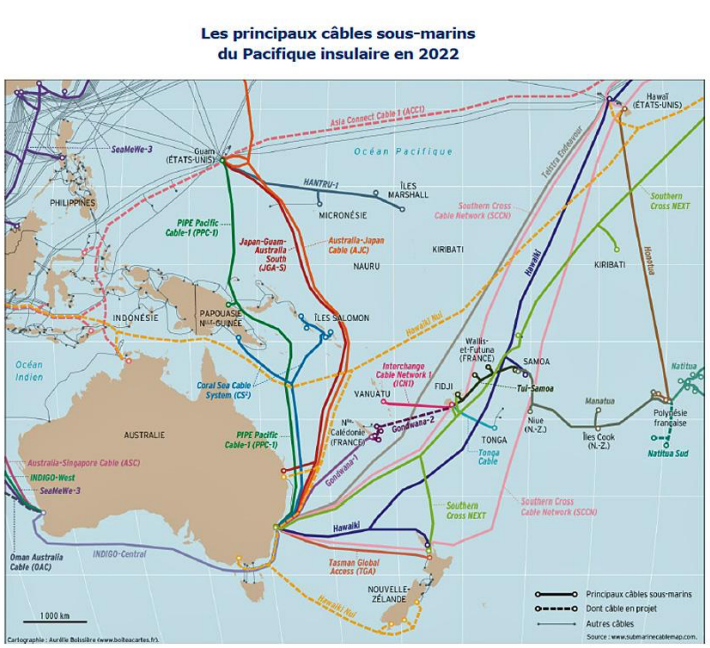
But, while cable breaks are not uncommon, repairs are complex, especially in contested or militarized areas. Repair vessels need secure access, international coordination and sometimes long lead times.

[3] https://millenniumprize.org/news-articles/news/supergraph-the-information-network-under-the-sea/

III. Why do geopolitical tensions make the problem worse?

Submarine cables are no longer just telecommunications infrastructure: they have become strategic assets at the heart of inter-state rivalries. In a context marked by the intensification of geopolitical tensions, their protection is now considered as a major national and international security issue. Their vulnerability can be exploited in the context of strategies of political pressure, sabotage or espionage, without an official declaration of armed conflict.

The rivalry between the US and China shows this trend. The two powers are seeking to strengthen their influence over global digital infrastructure, notably through the financing, construction and operation of new submarine cables. States are particularly concerned about the risks of espionage, technological dependence or foreign interference, which leads them to favor partners considered more reliable or to develop their own national capacities. Example:



The main submarine cables of the Pacific Islands in 2022

[4] Les câbles sous-marins en Océanie, un enjeu géopolitique de premier plan • TNTV News - Tahiti Nui Télévision

In 2021, the US, Japan and Australia announced funding for a submarine cable linking Nauru, Kiribati and the Federated States of Micronesia. Officially intended to improve the connectivity of these territories, the project also addressed geopolitical concerns, notably related to Huawei's participation. The US feared that an increased presence of Chinese business would strengthen Beijing's influence in this strategic region. This example illustrates how submarine cable projects have become part of power relations between great powers.

Geopolitical tensions amplify hybrid threats: cables become levers of strategic pressure, where espionage, technological influence and economic dependence combine.

In the face of these challenges, many states are seeking to strengthen their digital sovereignty, that is, their ability to control, protect, and secure their critical digital infrastructure. This strategy includes diversifying the routes used by submarine cables, reducing dependence on certain foreign suppliers, the development of national capacities for seabed monitoring and the strengthening of cooperation with partner States sharing the same strategic interests. However, this desire to secure critical infrastructure can also fuel international rivalries and make the establishment of global governance based on cooperation more complex.
Thus, geopolitical tensions are gradually transforming submarine cables into real power instruments. Their protection is no longer solely a matter of telecommunications, but is now a central issue of international security, economic stability and the preservation of state sovereignty.

IV. The consequences of an attack

A major attack or rupture of submarine cables could have major global consequences. Their failure would disrupt not only communications between states, but also the economy, essential services, and international security. A break in several cables could cause significant Internet slowdowns and even interrupt some international communications. Regions that depend on a limited number of cables would be particularly vulnerable, especially some territories in Africa, the Middle East or South Asia. Governments, businesses, hospitals and individuals could be affected.

The economic impact would be just as significant. According to this UN article, trillions of dollars in financial transactions pass through submarine cables every day. Banks, financial markets, international payment systems and e-commerce all rely on fast and secure data exchanges. Even a short-term downtime could slow down transactions, cause disruptions in financial markets, and undermine investor confidence. In a highly interconnected global economy, a localized outage can quickly have repercussions far beyond the affected area. A cut

in a strategic region, such as the Strait of Hormuz or the Suez Canal, could also affect shipping and global supply chains.

The consequences would also be significant on a military level. Armies use submarine cables to transmit information, coordinate their operations and command their forces. Communications between allies, intelligence systems, drone operations and military logistics rely partly on this infrastructure.

An attack on cables can thus directly affect states' digital sovereignty, limiting their ability to control essential communications and protect strategic data.

V. Conclusion

Commenté [1]: Pas la même couleuvre que le IV

An attack on the cables could therefore slow down the flow of information, complicate coordination between armed forces and reduce their ability to react quickly during a crisis or conflict. Finally, the sabotage of submarine cables poses a particular challenge: it is often very difficult to quickly identify those responsible. Unlike a typical military attack, a cable break can be caused by an accident, a natural phenomenon or an intentional act. This uncertainty complicates investigations and can fuel diplomatic tensions between states, each of which may interpret the origin of the incident differently. Thus, the protection of submarine cables is no longer just a matter for telecommunications. In a world where economies, states and societies are increasingly interconnected, cable protection has become an essential issue to ensure the continuity of global communications, economic stability and international security.

In summary, the protection of underwater cables requires a coordinated response from the international community, combining common standards, information sharing, enhanced surveillance, and cooperation between states and private companies. Without it, the security of global communications and the sovereignty of states will remain weakened in the face of hybrid threats.

ITU TREATIES AND MAJOR EVENTS

14/03/1884

Convention for the Protection of Submarine Telegraph Cables: this is the first treaty protecting cables. iscpc.org

16/11/1994

The United Nations Convention on the Law of the Sea (UNCLOS): It obliges states to protect cables and repair damage when they are at fault. Today, it remains the benchmark for states' rights and obligations regarding this infrastructure. (English: UNCLOS, French: CNUDM)

2008

The cutting of several cables connecting Europe, the Middle East and Asia has led to major communications and Internet disruptions in several countries, notably in India, Egypt and the Gulf States. This event highlights the strong dependence of states on these critical infrastructures.(www.euronews.com)

15/02/2023

After the sabotage of the Nord Stream[5] gas pipelines in September 2022, NATO created a coordination cell dedicated to critical underwater infrastructure (NATO maritime centre for the security of critical undersea infrastructure), whose mission is to map infrastructure vulnerabilities and coordinate Allied, partner and private-sector action.

2024-2025

Several telecommunications cables are damaged in the Baltic Sea in a context of high geopolitical tensions[6]. Although the origin of some incidents remains uncertain, these events recall the vulnerability of submarine cables to hybrid threats and highlight the need for enhanced international cooperation to protect this critical infrastructure.

[5] https://news.un.org/en/story/2023/02/1133752

[6] https://www.france24.com/en/live-news/20250114-nato-baltic-leaders-set-to-boost-security-after-cable-sabotage

POTENTIAL SOLUTIONS

1) Increase international cooperation to create more exchanges of information between States. For example, by creating a communication system that allows information to be shared quickly to prevent potential attacks, which would enhance the security of submarine cables.
2) Develop surveillance tools and improve existing ones to quickly detect suspicious activities, for example with underwater drones, sensors, or even artificial intelligence. (Examples on the NATO website)
3) Build several cable routes to avoid major problems due to a cut cable.
4) Increase cooperation between the States and private companies, since they own the majority of cables. Notably by sharing information on accidents, but also by helping each other (between public and private) to facilitate cable repairs, etc.
5) Find quick cable repair methods to limit the duration of restricted communication.

Some guided questions to help you with your research:

- How does your country position itself on the issue?
- What measures has your country already taken?
- Does your country have any allies who could be severely handicapped by the situation if a cable were to be cut?
- Does your country agree to form alliances with new partners?
- Does your country think it can ally itself with the private sector? (or does it want to have a power monopoly)

BIBLIOGRAPHY

- Gaur, Sachin: Invisible highways: The vast network of undersea cables powering our connectivity. 02.02.2026. URL: https://news.un.org/en/story/2026/02/1166867
- A new era of digital underwater communications. 27.04.2017. URL: https://www.nato.int/en/news-and-events/articles/news/2017/04/27/a-new-era-of-digital-underwater-communications
- The Conversation: Iran's threat to cut undersea cables in Strait of Hormuz poses a serious threat to Gulf states. 15.09.2026. URL: https://theconversation.com/irans-threat-to-cut-undersea-cables-in-strait-of-hormuz-poses-a-serious-threat-to-gulf-states-291618
- Euronews: What do we know about internet disruptions from cut subsea cables in the Red Sea. 08.09.2025. URL: https://www.euronews.com/2025/09/08/what-do-we-know-about-internet-disruptions-from-cut-subsea-cables-in-the-red-sea
- NATO:NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure. 28.05.2024. URL: https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui
- France24:NATO to boost Baltic Sea patrols after cable 'sabotage' blamed on Russia. 14.01.2025. URL: https://www.france24.com/en/live-news/20250114-nato-baltic-leaders-set-to-boost-security-after-cable-sabotage
- Supergraph: The Information network under the sea. 09.06.2022. URL: https://millenniumprize.org/news-articles/news/supergraph-the-information-network-under-the-sea/

- Câbles sous-marins de communication. 2022. URL: https://www.info.gouv.fr/upload/media/content/0001/10/ca2753fbe56d94423b50ccf54efb30d5f4e75672.pdf - Introduction to the subject
- Morel, Camille: La mise en péril du réseau sous-marin international de communication. 03.04.2020. URL: https://shs.cairn.info/article/FLUX1_118_0034/pdf?lang=fr - Describes various intentional attacks on the undersea telecommunications system (p.38).
- The Conversation: L'Iran menace les câbles sous-marins, ces artères invisibles d'Internet. 17.05.2026. URL: https://theconversation.com/liran-menace-les-cables-sous-marins-ces-arteres-invisibles-dinternet-283126 - Shows the vulnerability of cables and the consequences of an attack.

- TNTVNews: Les câbles sous-marins en Océanie, un enjeu géopolitique de premier plan. 13.09.2022. URL: https://www.tntvnews.pf/monde/les-cables-sous-marins-en-oceanie-un-enjeu-geopolitique-de-premier-plan/ - Describes the strategic and geopolitical importance of these facilities, located at the bottom of the oceans.
- Géoconfluences: Câbles sous-marins. 03.07.2023. URL: https://geoconfluences.ens-lyon.fr/glossaire/cables-sous-marins - History of cables and explanations of the dangers posed by cable damage.
- **Videos to help understand the issues related to submarine cables**

Mer baltique : la guerre hybride ? | L'Essentiel du Dessous des Cartes | ARTE
Géopolitique des câbles sous-marins | Géopoliticus | Lumni