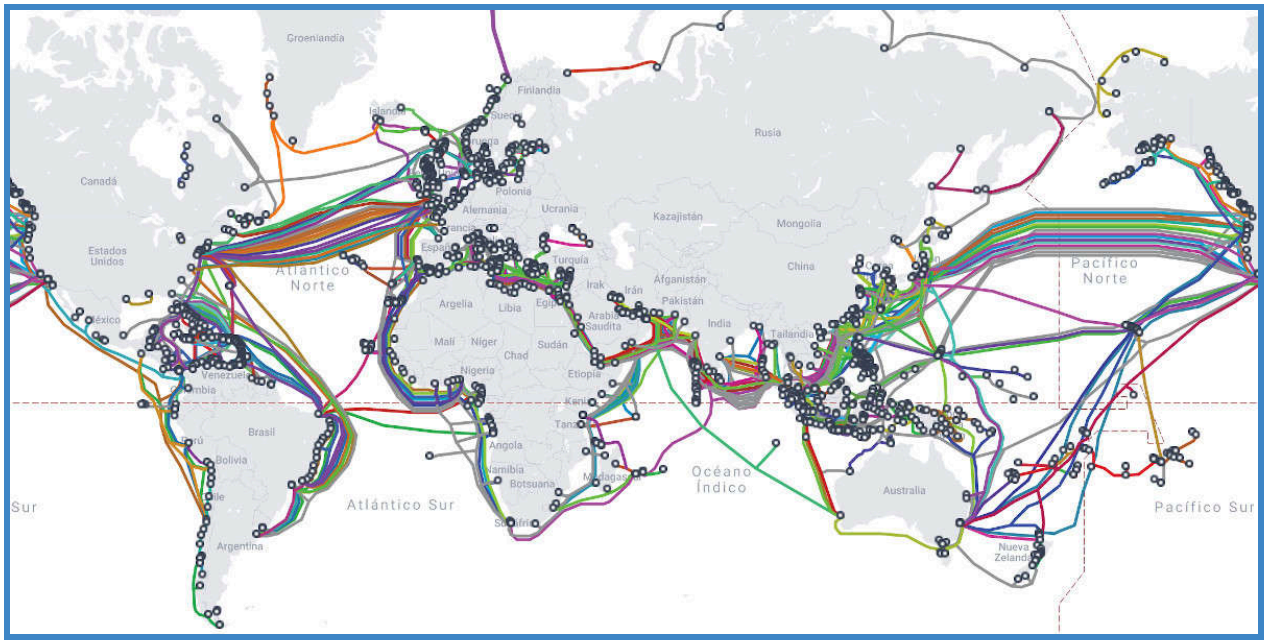

Undersea cable infrastructure paths (Universidad de Navarra)

The Protection of Undersea Infrastructures and Global Security

---

UNITED NATIONS SECURITY COUNCIL

April 2026

Head Chair: Helena Pelli

Co-Chair: Stella Teixera

TABLE OF CONTENTS

LETTER FROM THE DAIS

Dear Delegates,

It is our absolute pleasure to welcome you to the United Nations Security Council at MinasMUN 2026. My name is Helena Pelli, and alongside my Co-Chair Stella Teixeira, we will be guiding you through what promises to be a dynamic and challenging debate on The Protection of Undersea Infrastructures and Global Security.

Undersea cables and pipelines may not be visible in daily life, but they are the backbone of our modern world. Nearly all global internet traffic, financial transactions, diplomatic communications, and energy transfers depend on infrastructure lying silently on the ocean floor. Yet, as recent events such as the Nord Stream pipelines explosions have demonstrated, these systems are increasingly vulnerable to sabotage, hybrid warfare, and geopolitical rivalry.

As members of the Security Council, you will be tasked not only with understanding the technical and legal dimensions of this issue, but also with navigating the political tensions between major powers. Questions of sovereignty, militarization, cyberwarfare, private ownership, and international law will shape your negotiations. Remember that in this committee, diplomacy must balance national interests with collective security.

We encourage you to thoroughly research your country's maritime capabilities, alliances, economic dependencies, and stance on international law, especially the United Nations Convention on the Law of the Sea. Strong delegates will go beyond background information and propose realistic, enforceable solutions.

We look forward to seeing thoughtful debate, strategic alliances, and well-drafted resolutions. Do not be afraid to challenge ideas, respectfully, and defend your delegation's position with confidence.

We cannot wait to see the level of diplomacy you will bring to this chamber.

Sincerely,
Helena Pelli & Stella Teixeira
Chairs. UNSC

Head Chair:
Helena Pelli
helenafsampaiopelli@gmail.com
Escola Americana de belo Horizonte

Chair:
Stella Teixera
stellatxr2010@gmail.com
Escola Americana de belo Horizonte

COMMITTEE DESCRIPTION

Members of the UN Security Council sit during a meeting on Syria at the UN headquarters in New York City on April 5th 2017 (Shannon Stapleton)

The United Nations Security Council (UNSC) was established in 1945 following the adoption of the United Nations Charter, in the aftermath of the Second World War. Its creation reflected the international community's determination to prevent future global conflicts and to ensure a structured mechanism for maintaining international peace and security. Unlike other organs of the United Nations, the Security Council was designed to act swiftly and decisively in moments of crisis. It is the only UN body whose resolutions are legally binding upon all Member States, giving it unique authority within the international system.

The Council is composed of fifteen member states. Five of these are permanent members (China, France, the Russian Federation, the United Kingdom, and the United States) often referred to as the "P5." These states were granted permanent seats due to their roles as major powers at the end of World War II. In addition to the permanent members, ten non-permanent members are elected by the General Assembly for two-year terms, with seats allocated by regional representation. A defining feature of the Security Council is the veto power held by each permanent member, meaning that any substantive resolution requires not only at least nine affirmative votes, but also the absence of a veto from any of the P5. This

structure reflects the political realities of global power but also introduces complexity and diplomatic tension into decision-making processes.

The headquarters of the Security Council are located at the United Nations Headquarters in New York City, where ambassadors and representatives meet to deliberate on global crises. The Council's mandate, as outlined primarily in Chapters VI and VII of the UN Charter, allows it to investigate disputes, call for ceasefires, impose economic sanctions, establish peacekeeping operations, create investigative bodies, and, in extreme circumstances, authorize the use of force. Under Chapter VII specifically, the Council may determine the existence of a threat to international peace and security and take binding measures to address it.

Within this committee, delegates are expected to operate under the real constraints of international diplomacy. National interests, alliance systems, geopolitical rivalries, and the strategic use of veto power all shape negotiations. In the context of undersea infrastructure protection, the Security Council must assess whether acts of sabotage, cyber interference, or maritime disruption constitute threats to peace and security. Delegates must therefore balance sovereignty, international law, collective security, and military restraint while crafting realistic and enforceable solutions.

Topic A: The Protection of Undersea Infrastructures and Global Security

An underwater scene shoring large pipelines and cables running across the ocean floor. One appears to be damaged showing the vulnerability of the undersea infrastructure (New Civil Engineer)

BACKGROUND INFORMATION

Introduction

Undersea infrastructure are very critical systems that are located underneath or on the seafloor which include telecommunication cables, energy pipelines, gas pipelines and undersea power interconnectors.

Nowadays, about 99% of international data traffic is transmitted through more than 550 undersea fiber optic cables, covering over 1.4 million kilometers throughout the world. These cables are crucial for world communication, global banking transactions (10 trillion US dollars daily), diplomatic deals, military communication and internet globalization. Apart from the cables, the gas pipelines and electricity interconnectors are essential to energy security specially in Europe and East Asia.

Countries with the majority of energy and digital hubs are consequently the most affected, including the United States of America, Russia, Germany, China, United Kingdom, and Japan, also including maritime strategic points such as Norway and Turkey.

Although countries may discuss undersea infrastructure in terms of state security, a big portion of cable systems are owned and operated by private cooperation, such as google, meta, microsoft and amazon. They are primary global investors in these infrastructures, creating control challenges since critical infrastructure for national security is controlled by private cooperation rather than governments.

Because most infrastructure that connects the whole world lies on international waters, it is hard to legally protect and monitor these areas. Damage which can be accidental or on purpose can surely disrupt global communication and crucial markers, also affecting global security. In tense world conflict times, underwater infrastructure became an easy target for terrorism and sabotage that can in a quick action turn into a global crisis.

This debate directly relates to Chapter VII of the UN chatter which empowers the Security council to “determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.”

History

Initial Stage of Development

The first considered transatlantic telegraph cable was completed and installed on August 5 of 1858 and laid across the Atlantic again. This marked the beginning of submarine communications, with this first cable between the US and Britain. The first messages were sent on August 16th, however by October 20th of 1858, the cable stopped working. Despite the inconvenience, the Atlantic telegraph company did not give up its plans to connect two continents, and with the past problems in the next decade they built a successful cable to connect both places.

Impact during World Wars

During World War I, submarine cables were between the prioritized targets. In 1914 the United Kingdom cut Germany's transatlantic communications cables in the north sea, causing Germany to be isolated from the outside world, relying on wireless radio communication which were very easy to intercept. Consequently the British intelligence was able to monitor Germany's military plans contributing to many successful attacks and to the final outcome of the war.

In World War 2, undersea communication lines became even more critical, since they were important in coordinating troop movements across continents, naval operations and intelligence sharing. Both the Allies and the Axis strictly surveilled and protected their communications lines while trying to destroy the opponents lines. The war showed that the infrastructure was not just important for commerce but for strategic advantage in attack and defence.

Also during the Cold War, the cables allowed for the Soviet Union and the United States to sabotage each other with direct conflict, for example by stealing important data and intelligence communications.

Mainly, conflict shows that undersea infrastructure can be both an advantage and a weakness inheriting this vulnerability to today's world.

United Nations Convention on the Law of the Sea (UNCLOS)

In 1982 the UNCLOS established Maritime Zones and gave countries the responsibilities and rights of the underwater submarine cables that went through their determined Exclusive economic zone (EEZs). The problem is that this convention was held and negotiated before cyberconflicts were a problem, consequently not being up to date.

Globalization & Digital Spreading (1990s - 2010s)

During the 1990s, the world saw a rapid growth in internet usage, creating an even more dependent society on the fiber-optic submarine cables. PBy the early 2000s, military communications, international data diplomatic communications and financial transactions had increased significantly creating even more dependence. Private technology companies became the main investors in these cable systems, changing the main control stem from the state to corporate controlled infrastructure, making the government progressively more dependent on their private equities. Different from what most people think, Satellites are not the ones to carry the majority of the data. The cables carry almost all global internet traffic since they are more reliable, cheaper and faster.

Also during this time, Europe and Russia expanded their offshore pipeline networks since the demand for natural gas and energy increased significantly. The pipelines connecting Russia and Europe through the back sea and the Baltic became the center of europe;s energy security plan, but also increased dependency on these systems that can easily be sabotaged. The result was digital dependency on private owned cables while countries relied on undersea pipelines that cross many territories.

Vulnerability & Grey Zone Tactic (2014 - Present)

After Russia's annexation of Crimea in 2014, NATO started reassessing maritime threats in the Baltic and North Atlantic areas. With this annexation, the relations between Russia and Western countries started shattering, increasing tensions in the area, especially of gray zone tactics. Grey Zone tactics are strategies that allow the aggressor to cause gigantic damage to the economy or to a specific country while staying under the radar, maybe blaming the action on a natural accident. These can include cyberattacks, spread of misinformation, sabotage, and many more

On September 26 of 2022, the Nordstream pipelines were severely damaged with underwater explosions in the Baltic sea. The pipelines transported very important natural gas between Europe and Russia, being located in international waters but passing through EEZs of many countries. This increased the acknowledgement of the existing threat of sabotage of underwater infrastructure, especially when investigations came to be inconclusive, showing how a group can damage important structures without being detected.

This attack exposed gaps in surveillance and response capabilities, showing that a structure could be targeted without any military response. Since this attack, multiple cable disruption happened in the Baltic

and north sea regions, some attributed to accidental factors like anchor drags and some considered to be on purpose

Current Situation

The protection of undersea infrastructure has become a serious debate in today's world, especially with the build up of geopolitical rivalry between major powers. The infrastructure that was once viewed as simply commercial is now viewed as strategic key points to national security and intelligence

Because of the rising tensions all over the world, NATO has been increasing surveillance in the north atlantic and ballistic sea, with the goal to reduce sabotage and data stealing risks with rapid backfire if something happens. The European Union is also coordinating operations to focus on mapping all infrastructure and emergency repairs. China on the other hand is focusing on expanding their cable network with state companies which is slowly increasing their role in the digital era. Russia is specializing in naval vessels and deep sea explorating techniques which also raises concerns to the western countries.

The main concern is: when cables or pipelines are damaged or destroyed, it is almost always unclear if it was accidental or on purpose. This complicates diplomatic relationships and legal responses to these attacks, to which a country may hesitate to escalate the situation with a consolidated response. When tensions are high in the world, thai concern is even more relevant, since in a war situation, the infrastructure society relies on the most is on the list of the main targets to attack.

Along with that, a giant part of this infrastructure, specially the ones tied to western countries are privately owned. Governments therefore depend on their corporations for national defence and economic returns, possibly creating miscommunication or lack of cooperation threats.

Past UN Actions/Previous Attempts to Solve the Issue:

1982: Adoption of the United Nations Convention on the Law of the Sea (UNCLOS)

UNCLOS established the “laws” for governing a maritime zone, including territorial seas. Exclusive Economic Zones (EEZs) and the high seas. This guaranteed that cables and pipelines could be on the seafloor beyond territorial waters, but also reinforced and required that no state should intentionally damage any of these infrastructures. The EEZs allowed a country to have some sovereignty over the natural resources and energy infrastructure within their zone.

The concern is that UNCLOS was created before cyberwarfare, hybrid conflict and deep sea exploration technology had become common. Because the law lacks specific enforcement mechanisms that should come to act when it is broken, and does not treat the damage of undersea infrastructure as an international law issue, the implementation of UNCLOS depends on the government's good will to follow it, creating inconsistencies and numerous violations.

2008-2015: United Nations Security Council Resolutions on Maritime Security

During this period of time, the Security Council came up with multiple resolutions to address privacy concerts on the coast of Somalia and other ocean security threats. This resolution simply increased naval cooperation, UN anti-piracy operations and the protection of commercial shipping routes.

Even though these resolutions were not focused on undersea infrastructure protection, these actions could represent that the Security Council recognized that maritime threats are a real issue to international security and peace. Furthermore, they established efforts for coordinated naval patrols and information sharing mechanisms, which could significantly increase security in the seas. But, these efforts are not even close to addressing the security of undersea infrastructure, since they are a much more complex issue

2013 - Present: UN Cybersecurity Concerns

The UN group of governmental experts (GGE) and the Open-Ended Working Group (OEWG) debated the state's behavior in cyberspace. The discussions basically consisted of emphasizing the protection of infrastructure from cyberattacks and reinforced that digital systems are more than important to national security and stability

Even though this was mostly focused on cyberattacks rather than physical protection of infrastructure, the debates are very relevant since the cables share the physical space of global internet space. A cyberattack could include messing with the cable management systems, producing similar effects to a direct attack on a cable. But, no agreement has been made to protect important infrastructure in both physical or digital spaces.

2022 - 2024: Infrastructure Protection General Assembly

After the 2022 delegate to the Nord Stream pipelines, several states raised concerns inside the general assembly about the vulnerability of these infrastructure, both communicational and energetic. The debates discussed risks of sabotage, hybrid warfare tactics such as grey zone tactics, and difficulty of security in the environments where the infrastructure is located

Even though the discussion happened, division of position among the major powers has not allowed the UNSC to create a resolution to directly address the security and protection of undersea infrastructure. As a result, positions are fractured and interests remain more regional rather than international.

POSITION OF MAJOR BLOCS

United States of America

The United States views undersea infrastructure as crucial for both national and international security, but also to all kinds of trade and communication in the world. Being a central hub in the global digital economy, the US has various cables that carry military communication , intelligence data, financial transactions, etc. A large amount of global undersea cables are financed or owned by US technology companies, which places the country in a position where its private corporations are in control of national security

Washington worried that possible opponents could use their underwater capabilities to target cables and pipelines in times of peace, consequently causing a reaction, creating conflict. The US supports that countries have awareness of what is happening within their sea borders, that intelligence is shared and that NATO coordinates strategies to protect cables by using cable redundancy throughout cable routes.

The US must balance their need for security in these areas with their long term advocacy for freedom of navigation and open seas. They would advocate for cooperation and both public and private partnerships between nations, but be against restricting data flow.

Russian Federation

Russia's undersea infrastructure is a sovereignty, security and economic issue. As a major exporter of natural gas with pipelines in the Baltic, Arctic and black Sea, Russia strongly depended on offshore pipelines to sell their product to other countries, specially Europe, At the same time, Russia has been strongly accusation of developing then own technology for deep sea operations, seen a threat to western nations.

After the damage to the Nord Stream pipelines in 2022, Russia said that they were a victim of infrastructure sabotage and wanted independent investigation . It stance was that NATO should not be expanding its surveillance or military presence in Russian maritime zones

Russia would likely stand with the UNCLOS, which included non interference in sovereign states. Also , they would oppose any proposal that increases surveillance or NATO military presence near their borders, likely arguing that no accusations should be made without concrete proof, and that these usually target Russia.

People's Republic of China

China plays a key role in investing and building undersea cable systems around the world. Projects like the Digital Silk road help finance and construct cables inside the oceans connecting Africa, Europe and Asia.

Since China depends on global trade and digital communication, it will strongly support secure and stable undersea infrastructure. However, if that involves the military, then China would probably not support it. China prefers cooperation inside the United Nations with international law rather than having western-lead military presence near its shores.

China would argue that security of undersea infrastructure should be seen as an excuse to militarize certain regions. It may support dialogues and shared responsibilities to develop coalitions to the problem without military intervention. However, at the same time, China at all costs will protect its own strategic interest, especially in the South China Sea where Taiwan is located.

United Kingdom of Great Britain and Northern Ireland

The United Kingdom is vital to the global submarine cable network, connecting itself to Europe and North America, making it a key communication hub. As a member of NATO, the UK is concerned about the severe risk of sabotage of the pipelines and undersea cables,which could severely disrupt economic and communications systems. The country has increased surveillance and naval patrols near its cable waters. The UK mainly views these cables as part of an important national defence system and vital to Europe's security

Inside the date, the UK will mainly support cooperation between allies and intelligence sharing. Also, it will advocate for better systems for investigation of accidental or on purpose damage. At the same time,

the UK will continue to support freedom of navigation and international maritime law, keeping solutions within that frame.

Federal Republic of Germany

Germany position has been very influenced by the damage of the Nor Stream pipelines in 2022, As one of Europe's largest economies, Germany depends heavily on stable energy supplies usually coming from the pipelines and secure communications from the cable systems

After the incident, Germany focused more on diversifying its energy sources, especially with the Russia and Ukraine war. Also, it has improved its infrastructure protection close to its shores. Germany will support European cooperation and better monitoring of vital infrastructure, however, without escalating tensions and keeping things always diplomatic.

Germany will support better international investigations and transparency, with systems that countries can rely on to judge if an accident was on purpose or by accident. Germany will also likely avoid harsh language to avoid conflict and be more on the side of cooperation, long term security and stability

Kingdom of Norway

Norway is Europe's biggest supplier of natural chassis and has many offshore energy platforms in the North Sea. Norway is also a very important strategic point on the map because of its strategic location in the north sea. Because a large part of its economy depends on energy exports, the protection of these infrastructure is vital to the country

After 2022's reports of drone activity near offshore energy platforms, Norway increased security patrols and monitoring around its infrastructures. As a NATO member sharing a border with Russia in the arctic circle, Norway views protection as crucial for stability and national security.

Norway will advocate for enhanced maritime surveillance with rapid response mechanisms to any attacks with NATO coordination. However, because it is an important but smaller state, it emphasizes that sticking to peace and to international law is a crucial step. Norway would also promote transparency and communication in situations of crisis, since it is highly vulnerable to maritime related activities

French Republic

France has one of the largest maritime zones in the world because of its various overseas territories around the world. This means that it has many submarine cables and energy systems under its control and territory. Frece sees this infrastructure as a very important part of national sovereignty and Europe's security.

Since France is a permanent member of the Security Council, it will support strong international cooperation within international law. France would also likely support better monitoring systems, clear laws about consequences to sabotage and cooperation between countries and private companies. However, it would also emphasize that military escalation would be unnecessary between major powers, promoting solutions led by the United Nations rather than just based on alliances.

TIMELINE OF EVENTS

Date	Description
1982 – Adoption of the United Nations Convention on the Law of the Sea (UNCLOS)	In 1982, the United Nations Convention on the Law of the Sea (UNCLOS) was adopted, establishing the legal framework governing maritime zones, including territorial seas, Exclusive Economic Zones (EEZs), and the high seas (6). UNCLOS allows states to lay submarine cables and pipelines on the seabed beyond territorial waters and obliges states not to intentionally damage such infrastructure. However, the convention was drafted before the rise of cyberwarfare, hybrid conflict, and deep-sea surveillance technologies. While it provides foundational legal protection for undersea infrastructure, it lacks specific enforcement mechanisms and does not clearly define sabotage of submarine cables as a direct act of aggression. This legal gap is central to current debates within the Security Council.
1990s–2000s – Rapid Digital Globalization	During the 1990s and early 2000s, the expansion of the internet dramatically increased global dependence on submarine fiber-optic cables. Today, approximately 99% of international data traffic travels through more than 550 undersea cables (1). These systems became essential for financial markets, military communications, diplomacy, and global commerce. Unlike satellites, submarine cables provide faster, cheaper, and more reliable data transmission. During this period, private technology corporations began investing heavily in cable systems, shifting ownership from governments to companies. This privatization introduced new governance challenges, as infrastructure critical to national security became largely corporate-controlled. The digital globalization era transformed submarine cables from commercial assets into strategic infrastructure vital to global stability.

2008–2015 – UNSC Maritime Security Resolutions	Between 2008 and 2015, the United Nations Security Council adopted several resolutions addressing maritime security threats, particularly piracy off the coast of Somalia (8). These resolutions increased naval cooperation, intelligence sharing, and multinational patrols to protect shipping routes. Although they did not specifically address undersea infrastructure, they demonstrated the Security Council's recognition that maritime threats can constitute risks to international peace and security. These resolutions also established frameworks for coordinated naval presence and joint security mechanisms. However, submarine cables and pipelines remained largely unaddressed, revealing a policy gap between protecting visible maritime trade routes and safeguarding hidden but equally critical infrastructure on the ocean floor.
2014 – Russia's Annexation of Crimea	In 2014, Russia annexed Crimea, significantly escalating tensions between Russia and Western powers. Following this event, NATO began reassessing maritime security threats in the Baltic and North Atlantic regions. Concerns emerged regarding "grey zone" tactics, actions that fall below the threshold of open warfare but destabilize adversaries. Submarine cables and pipelines became increasingly viewed as potential targets of hybrid warfare strategies. This period marked a shift in perception: undersea infrastructure was no longer seen merely as economic assets but as vulnerable components in geopolitical competition. NATO increased surveillance activities in strategic maritime areas, raising debates over militarization versus sovereignty.
2022 – Nord Stream Pipeline Explosions	On September 26, 2022, the Nord Stream pipelines were severely damaged by underwater explosions in the Baltic Sea (7). These pipelines transported natural gas between Russia and Europe and were located in international waters while passing through multiple EEZs. Investigations into the incident were inconclusive, and responsibility remains disputed. The attack exposed major vulnerabilities in undersea infrastructure

	protection and raised concerns about the ability of states to detect and attribute sabotage. It also demonstrated how damage to energy infrastructure could have massive geopolitical and economic consequences. The event intensified global awareness of the risks facing submarine infrastructure and directly connects to current UNSC debates.
2023 – Increased NATO and European Surveillance	Following the Nord Stream incident, NATO members increased naval patrols and surveillance in the North Sea and Baltic regions. The United Kingdom and Norway announced joint naval patrols to protect undersea infrastructure (13). European states also signed pledges to enhance monitoring of critical maritime systems (14). These measures aimed to deter sabotage and improve rapid response capabilities. However, increased military presence in strategic waters also raised tensions with Russia, which opposed expanded NATO surveillance near its maritime borders. This development highlights the balance between collective security efforts and risks of escalation.
2023–2024 – Growing Concerns Over Cable Disruptions	Between 2023 and 2024, multiple submarine cable disruptions were reported in the Baltic and North Sea regions. While some incidents were attributed to accidents such as anchor drags, others raised suspicions of deliberate interference. Reports of drone activity near Norwegian offshore energy platforms further increased security concerns (9). These incidents reinforced the difficulty of distinguishing between accidental damage and intentional sabotage. The lack of clear attribution mechanisms complicates diplomatic responses and increases the risk of miscalculation. This ongoing uncertainty has strengthened arguments within the UN that existing legal frameworks are insufficient to address modern hybrid threats.
2024 – Renewed Global Debate on Infrastructure Protection	By 2024, protection of undersea infrastructure had become a major topic in international security discussions. The United Nations General Assembly saw increased debate regarding hybrid warfare and infrastructure vulnerability. Meanwhile, major powers such as the United

	States, China, and Russia expanded investments in maritime surveillance and deep-sea capabilities. The absence of a comprehensive international agreement specifically addressing submarine infrastructure protection has left states divided. The issue now sits at the intersection of sovereignty, cybersecurity, militarization, and private corporate control, making it highly relevant for action by the Security Council.

DEFINITION OF KEY TERMS

Undersea Cables

Fiber-optic cables laid on the ocean floor that transmit nearly all global internet and telecommunications data.

Exclusive Economic Zone (EEZ)

A maritime zone extending 200 nautical miles from a coastal state, where the state has sovereign rights over natural resources under the United Nations Convention on the Law of the Sea.

Hybrid Warfare

A strategy combining conventional military force with cyberattacks, misinformation, sabotage, and economic pressure.

Grey Zone Tactics

Actions that fall below the threshold of traditional war but aim to destabilize or damage another state.

Critical Infrastructure

Systems essential to a country's security, economy, and public safety.

NATO

The North Atlantic Treaty Organization, a military alliance focused on collective defense.

Chapter VII (UN Charter)

Section of the United Nations Charter that allows the Security Council to take binding measures in response to threats to peace.

FURTHER RESEARCH

1. United Nations - UN Charter (Chapter VII):

   https://www.un.org/en/about-us/un-charter/chapter-7

2. United Nations Convention on the Law of the Sea:

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

3. International Cable Protection Committee:

   https://www.iscpc.org/

4. NATO - Maritime Security:

   https://www.nato.int/

5. Security Council Report:

   https://www.securitycouncilreport.org/

6. Reuters coverage of the Nord Stream pipelines incident:

   https://www.reuters.com/

GUIDING QUESTIONS

- To what extent should undersea infrastructure be considered a matter of collective security rather than national sovereignty?
- Should the Security Council authorize enhanced maritime surveillance, even if it increases military presence in contested regions?
- How can the UN distinguish between accidental damage and deliberate sabotage in international waters?
- Should private technology companies be legally required to coordinate security strategies with governments?
- Is existing international law, particularly UNCLOS, sufficient to address modern cyber and hybrid threats?

WORKS CITED

1. Invisible highways: The vast network of undersea cables powering our connectivity | UN News
2. Optical Core Infrastructure: The Hidden Highway of Connectivity | Wilson Center
3. To keep the world's data flowing, countries need to quickly fix broken undersea cables
4. Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Articles 39-51) | United Nations
5. The first transatlantic telegraph cable 1858
6. United Nations Convention on the Law of the Sea
7. What is known about the Nord Stream gas pipeline explosions? | Reuters
8. UN Documents for Maritime Security
9. Unidentified drone spotted over Norwegian gas field, police investigating
10. Subsea Cables and US National Security
11. Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition
12. US and its Allies Issue Joint Statement on the Security and Resilience of Undersea Cables
13. UK and Norway will mount joint naval patrols to protect undersea cables and hunt Russian submarines | AP News
14. European states sign pledge to protect North Sea infrastructure
15. International Cable Protection Committee
16. United Nations Convention on the Law of the Sea - Wikipedia
17. The changing submarine cables landscape | European Union Institute for Security Studies
18. Policy Brief: Enhancing the Resilience of Submarine Internet Infrastructure
19. The AI Economy's Massive Vulnerability
20. How vulnerable are undersea cables? | Network World
21. Submarine communications cable - Wikipedia
22. Red Sea Cable Cuts: Envisaging Operational Framework for Securing Critical Undersea Infrastructure - MP-IDSA
23. 2Africa - Wikipedia
24. Sweden signs Memorandum of Understanding on the protection of critical undersea infrastructure - Government.se
25. G7: Declaration by Foreign Ministers on the Maritime Security and Prosperity | EEAS
26. NATO's maritime activities | NATO Topic
27. NATO launches 'Baltic Sentry' to increase critical infrastructure security
28. Joint press conference | NATO Transcript

29. Joint Statement of the Baltic Sea NATO Allies Summit - President
30. ‘Without Maritime Security, There Can Be No Global Security’, Secretary-General Tells Security Council, Calling on Greater Respect for International Law