MESMUN’26

International Telecommunication Union Crisis Committee

STUDY GUIDE

Agenda Item:

Attack on Global Telecommunications Infrastructure

Table of Contents

1. Letters

Letter from Secretary-General

Dear Delegates of the ITU Committee,

It is my pleasure to welcome you all to MESMUN'26. On behalf of the MESMUN'26 team, I extend my warmest greetings to each and every one of you, our dear participants. We wish you a productive and engaging experience.

The International Telecommunication Union (ITU) plays a vital role in ensuring the stability, accessibility, and security of global communications networks. In a world where connectivity between individuals is increasing, telecommunications infrastructure is a very important pillar of modern society, allowing society to unite from anywhere in the world, while supporting global finance, security and governance systems as well.

The agenda item, "Attack on Global Telecommunication Infrastructure," addresses a highly relevant and urgent issue in contemporary international security. The sabotage that occurred has had a daunting effect globally. Disruptions in various systems have caused widespread confusion, panic, and consequences, such as economic instability, cutting international communication, and harming global security.

As delegates, we expect you all to approach this topic with a sense of responsibility, analytical and quick thinking, and awareness of your surroundings. This might as well be a race against time, and you, our esteemed delegates, are tasked with stopping further damage.

I encourage all delegates to actively participate in discussions, respect different viewpoints, and work collaboratively towards solutions that will not only help your country but help the globe.

I wish you all the best in your discussions and hope this experience will improve you as a person.

Yours sincerely,
Toprak PERÇİMLİ
Secretary General
MESMUN'26
percimlit@gmail.com

Letter from Under Secretary-General of ITU

Dear Delegates,

I am very glad to welcome you to the International Telecommunication Union Crisis Committee at MESMUN 2026.

The topic we will be working with—an attack on global telecommunications infrastructure—might sound technical at first. It is not. At its core, it is about disruption. When communication networks go down, everything else follows. Financial systems stall, governments lose coordination, and basic services start to break apart. That is the kind of pressure this committee is built around.

Crisis committees tend to feel different from standard MUN. Things move faster. You will not always have time to prepare the perfect response, and often you will be working with incomplete information. That is part of the experience. What matters more is how you think in the moment. Can you stay clear, make decisions, and adjust when the situation shifts? That is what will shape your performance here.

The study guide is there to help you get started. It gives you the structure, the background, and the key ideas you will need. But it will not carry you through the committee on its own. The delegates who stand out are usually the ones who go a bit further. They understand their role properly, think about what could go wrong before it happens, and come in ready to act rather than wait.

At the same time, do not overcomplicate this. You are not expected to have perfect answers. This committee is also about figuring things out as you go, testing ideas, and improving as the sessions progress. If you are engaged and thinking seriously about what you are doing, you are already on the right track.

If anything is unclear while you are preparing, feel free to reach out.

Email: adityaadiaj1234@gmail.com

I am looking forward to seeing how each of you approaches the committee.

Yours sincerely,
Aditya Jindal
Under-Secretary-General

2. Introduction to the Committee

2.1 What is a Crisis Committee?

A crisis committee is a dynamic, simulation-based form of Model United Nations in which delegates are not merely representatives of member states engaged in long-form resolution drafting, but active decision-makers responding to an evolving, high-stakes international emergency in real time. Unlike traditional General Assembly committees, where proceedings are structured around a fixed agenda and cumulative resolutions, a crisis committee operates under the constant pressure of a shifting situation — one that responds directly to the actions, directives, and failures of the delegates themselves.

In this committee, delegates represent specific roles within the international telecommunications and governance ecosystem, acting within the authority, responsibilities, and limitations that those roles carry. The emphasis throughout will be on practical problem-solving, coordinated response, and realistic decision-making — not abstract policy positions.

The principal tool through which delegates act is the directive. Directives are written action documents submitted to the Committee leadership for evaluation and response. They may be collective in nature — reflecting the coordinated will of the Committee — or confidential and role-specific. The outcomes of directives are communicated back to delegates through crisis updates, which introduce new developments, escalations, and consequences into the scenario, requiring delegates to continuously adapt their strategy. Alongside directives, delegates may submit Information or Expert Requests to obtain technical clarifications, risk assessments, or data relevant to the crisis at hand.

Debate in this committee will proceed primarily through Semi-Moderated Caucuses, in which delegates speak in a structured format on a defined topic, and Unmoderated Caucuses, which allow for free movement, coalition-building, and directive drafting. There is no General Speakers' List. Proceedings are designed to remain fast-paced, immersive, and solution-oriented.

A Crisis Orientation will be conducted at the opening of the first session by the Committee leadership, covering directive mechanics, debate procedure, and the flow of crisis updates in detail.

For the complete procedural framework governing this committee — including the standards for directives, the full list of motions and points in order, voting thresholds, and the authority of the Committee leadership — delegates are strongly encouraged to read the

Official Rules of Procedure of the ITU Crisis Committee at MESMUN'26, which has been separately published and distributed.

2.2 Introduction to the International Telecommunication Union

The International Telecommunication Union — the ITU — is the United Nations specialized agency responsible for digital technologies and global communications, and one of the oldest international organizations in existence. Its membership includes 194 Member States alongside more than 1,000 companies, universities, research institutes, and regional and international organizations, making it one of the most broadly represented technical bodies in the entire UN system.

The ITU's core functions fall into three areas. It coordinates the global use of radio spectrum and satellite orbits, ensuring that different countries and operators do not interfere with each other's communications. It develops international technical standards that allow equipment and systems built in different countries to work together. And it supports digital development and connectivity, with a particular focus on developing countries and underserved regions.

Beyond these standard functions, the ITU plays an operationally important role in emergency communications — one that is directly relevant to this committee. Its emergency-telecommunications work includes support for National Emergency Telecommunication Plans, the Disaster Connectivity Map, and implementation support tied to the Tampere Convention on disaster-relief communications. The Disaster Connectivity Map alone had been activated in more than 80 countries and disaster events as of January 2026.

2.3 Introduction to the Agenda Item

Global telecommunications infrastructure is not a single network. It is a layered system of interconnected components that together carry the world's data, financial transactions, communications, and emergency services. The ITU breaks this system into three layers: the first mile, where international connectivity enters a country through submarine cables, satellite links, landing stations, and cross-border systems; the middle mile, which includes national backbones, internet exchange points, data centres, cloud platforms, and content-delivery networks; and the last mile, which connects individual users through fibre, mobile networks, fixed wireless, or satellite access.

At the centre of this system are submarine fibre-optic cables. More than 99 per cent of international data traffic travels through a network of approximately 500 submarine cables

spanning over 1.7 million kilometres worldwide. A significant disruption to these cables does not only affect internet browsing — it ripples across financial systems, hospital communications, government services, airlines, military institutions, and the basic functioning of modern economies. Understanding the architecture of this system, the threats it faces, and the legal and institutional tools available to respond is the foundation of effective participation in this committee.

3. Historical and Institutional Background

3.1 Origins and Evolution of the ITU

On 17 May 1865, twenty founding states signed the first International Telegraph Convention in Paris, establishing the International Telegraph Union — the earliest form of the modern ITU. The founding purpose was direct: standardize cross-border telegraphy and make international communication interoperable. Before the Convention, a message sent from one country could not travel through another's telegraph network if the two systems used different technologies or codes; the ITU was created to solve that problem.

This founding logic — using common rules and technical coordination to address transnational communications challenges — has defined the ITU throughout its history. From telegraphy, its mandate expanded to telephony, then to radiocommunications and satellite coordination, and eventually to the governance of the digital age. The organization was formally integrated into the United Nations system after the Second World War and took its current name in 1934.

For delegates, this history carries a practical implication. The ITU was not built to act as an enforcement body or a military authority. It was built to facilitate coordination, develop shared standards, and bring governments and private actors to the table. These qualities are both its most important strength and its clearest limitation when facing the kind of crisis this committee addresses.

3.2 The Development of Global Telecommunications Infrastructure

For most of the twentieth century, telecommunications infrastructure was built, owned, and managed primarily by governments. National telephone companies — in many countries state monopolies — controlled domestic networks, while international connectivity was handled through state-to-state agreements and intergovernmental bodies. The ITU played a central regulatory role in this environment.

That model shifted significantly in the 1990s, when telecommunications markets were progressively privatized and the internet expanded rapidly. Private companies took over the construction and operation of both national and international infrastructure, and today the majority of the world's most critical connectivity assets — including most submarine cable systems — are owned and operated by private entities rather than states.

Investment in this infrastructure has accelerated sharply in recent years. ITU's 2025 connectivity reporting records submarine cable investment rising from USD 0.8 billion in 2015 to USD 9.7 billion in 2025. A growing share of this investment now comes from large

technology companies — hyperscalers such as Google, Meta, Microsoft, and Amazon — that have become major financiers of new cable systems to support their global cloud and data operations. This shift from a state-regulated environment to one shaped by private capital and large technology firms is one of the defining features of the current governance landscape; it also creates real challenges for the kind of coordinated international response this committee must produce.

4. Architecture of Global Telecommunications Infrastructure

4.1 Submarine Fibre-Optic Cable Systems

Submarine cables are the physical foundation of global internet connectivity — long fibre-optic cables laid on or beneath the seabed, transmitting data as pulses of light across oceans and continents at very high speeds.

Each cable system has two main parts. The wet plant is everything submerged: the cable itself, the repeaters that boost signal strength over long distances, and the branching units that allow the cable to split and connect to multiple endpoints. The dry plant covers the shore-based equipment — transponders, power-feed systems, and monitoring hardware — located at cable landing stations on land.

These systems are built to last approximately 25 years or more. However, because they run across vast distances of open ocean, they are physically difficult and expensive to repair when something goes wrong. A repair vessel must be sent to the precise location of the fault — a process that can take days or weeks — and accessing certain areas requires permits from multiple governments along the route. The concentration of so much of the world's data traffic on these physical cables is precisely what makes their protection a matter of international strategic importance.

4.2 Cable Landing Stations and Terrestrial Backhaul

A cable landing station is the facility where an international submarine cable comes ashore and connects to a country's domestic network. Located near coastlines, these stations serve as the entry point through which all international internet traffic flows into a country — and from which it travels onward through terrestrial infrastructure, including long-distance fibre cables and transmission systems, out to cities, institutions, and homes.

Landing stations are critical nodes. If a station is damaged, loses power, or is otherwise disabled, the submarine cables connected to it become effectively unusable — even if the cables themselves are entirely intact. This makes landing stations a high-priority target in any scenario involving deliberate infrastructure attack, and a high-priority subject in any resilience planning that takes physical security seriously.

4.3 Internet Exchange Points, Data Centres, and Cloud Systems

Three types of infrastructure shape the middle mile of global telecommunications: internet exchange points (IXPs), data centres, and cloud platforms.

An internet exchange point is a physical location where different networks connect and exchange data traffic. IXPs keep local internet traffic within a country rather than routing it through distant international servers — reducing costs, improving speed, and significantly strengthening resilience. When an international cable is damaged, traffic exchanged and hosted locally can continue to flow without interruption, because it never needed the international cable in the first place.

The April 2024 outage of the SEA-ME-WE-5 submarine cable affecting Bangladesh makes this point clearly. Despite the cable damage, traffic at Bangladesh's internet exchange point dropped only marginally, because much of the country's most used web content was already hosted domestically. Countries with no local hosting capacity face the opposite outcome: a single cable break can produce near-total loss of international connectivity. Data centres and cloud platforms reinforce this same logic — the more content a country hosts locally, the less dependent it is on uninterrupted international links.

4.4 Satellites as a Complementary Layer

Satellite internet provides a valuable backup option, particularly for remote regions and island states with limited or no alternative international connections. When submarine cables are disrupted, satellites can help maintain some level of connectivity.

However, satellites cannot fully substitute for cable systems at current levels of global demand. The global number of satellite subscriptions remains extremely low — less than one per 1,000 inhabitants worldwide, according to ITU's 2025 reporting. The capacity, speed, and cost limitations of satellite systems mean they function as a complementary layer rather than a reliable mass failover. For the purposes of this committee, satellite connectivity is best treated as a partial and temporary measure: useful for keeping emergency communications and critical services minimally functional while cable repairs proceed, but not a solution in itself.

4.5 Chokepoints, Route Diversity, and Systemic Vulnerability

Not all countries face the same level of risk from a submarine cable disruption — and the difference is largely determined by decisions made long before any fault occurs.

Route diversity means having multiple different cable paths between countries and regions, so that if one route is damaged, traffic can shift to another. Redundant landing points mean cables arrive at more than one location on a coastline, so damage to one station does not cut off an entire country. When cables cluster at the same landing points or follow the same geographic corridor, they create chokepoints — locations where a single incident can affect multiple cables at once, dramatically multiplying the scale of disruption.

The ITU's Working Group 2 recommendations call for routine stress tests to assess chokepoint and route congestion risks, alongside requirements for route diversity, redundant landing points, repair agreements, spare cable stock, and enhanced security at cable stations. The underlying message is clear: resilience is not simply a function of how many cables exist, but of where they go and how readily traffic can be rerouted when something goes wrong.

5. The Threat Landscape

5.1 Accidental Damage and Natural Hazards

The most common cause of submarine cable damage is accidental — not sabotage or cyberattack. The ITU and the International Cable Protection Committee record approximately 150 to 200 cable faults globally each year, requiring roughly three repairs per week. The leading causes are fishing vessels dragging equipment across the seabed and ships dropping anchor in areas where cables run. ITU's 2025 reporting puts the share of faults attributable to these types of human activity at 86 per cent.

Natural hazards account for a smaller overall share, but they can cause severe damage when they strike. Earthquakes, submarine landslides, storm surges, cyclones, volcanic eruptions, floods, and — in polar regions — ice scour can all damage cables and landing stations. These events are particularly dangerous because they can affect multiple cables simultaneously in the same area, without warning and with no possibility of coordinated prevention.

For this committee, the baseline level of accidental damage has a direct practical implication. Any crisis response mechanism must be capable of distinguishing ordinary accidental faults — which are routine events managed through standard repair channels — from incidents that suggest something more serious. That distinction is harder to draw in practice than it sounds.

5.2 Physical Sabotage and Hybrid Threats

Deliberate physical sabotage is an increasing concern, particularly in the context of geopolitical tension. What makes this threat especially difficult to manage is that intentional sabotage — carried out using anchor dragging or similar methods — can be nearly impossible to distinguish from accidental damage in the immediate aftermath of an incident. The same physical mark on a cable can be left by a careless fishing vessel or a deliberate act; the difference lies in intent, not evidence.

Recent events in the Baltic Sea have brought this problem into sharp focus. In January 2025, damage to a fibre-optic cable between Latvia and Sweden triggered a formal sabotage investigation and the deployment of NATO patrol forces. These events were part of a broader pattern of incidents affecting cables and energy infrastructure in the region — a pattern serious enough to prompt NATO to launch its Baltic Sentry programme in January 2025, specifically dedicated to protecting critical undersea infrastructure.

These developments mark a shift in how states and international organizations are beginning to treat cable security: no longer as a purely technical maintenance and repair

challenge, but increasingly as a security, attribution, and deterrence problem that requires military awareness, legal investigation, and active surveillance.

5.3 Cyber-Physical Exposure

A third category of threat has received growing attention in recent policy discussions: the vulnerability of the control systems and digital interfaces that manage submarine cable infrastructure.

Submarine cables are not passive physical assets. They are controlled, monitored, and managed through software systems at cable landing stations and network operations centres — systems that are themselves vulnerable to cyberattack. A successful intrusion into these command-and-control systems could, in principle, allow an attacker to disrupt or manipulate cable operations without ever physically touching a cable. The ITU's 2026 Working Group 2 recommendations explicitly call for security audits and stress tests of cable stations, digital access portals, and outside plant systems. Protecting the physical cable, in other words, is not sufficient — the entire cyber-physical system that operates it must be hardened against interference as well.

5.4 Governance Fragmentation and Private Ownership

The most structurally significant challenge in the threat landscape is not a specific attack type — it is the governance problem that shapes the response to all threats.

Most of the world's submarine cable infrastructure is privately owned. As TeleGeography has noted, cables are generally built, owned, and maintained by private entities, with direct public investment remaining rare. The growing involvement of hyperscalers — Google, Meta, Microsoft, and Amazon — as major cable investors has deepened this pattern considerably. The result is a fundamental mismatch: telecommunications infrastructure is strategically public in its importance — economies, governments, hospitals, and militaries depend on it — yet largely private in its ownership and governance. When a crisis strikes, states bear the political responsibility for public safety and connectivity, but they do not always hold direct authority or operational control over the assets involved. Bridging this gap between public responsibility and private ownership is one of the central governance challenges this committee must confront.

6. The Crisis Scenario

6.1 The Specter Incident and Its Immediate Consequences

In the first quarter of 2026, simultaneous damage was detected in submarine fibre-optic cables across multiple continents. The damage was not concentrated in a single region but spread across several major cable corridors — a pattern inconsistent with accidental causes and strongly suggestive of coordination.

The consequences were immediate and cascading. Internet connectivity was disrupted across several regions. Financial transactions were delayed; military and government communications were interrupted; airlines faced operational difficulties; access to global social media platforms was restricted in affected areas; hospitals and government portals experienced significant disruption. Technical investigations conducted in the days following the incident ruled out ordinary wear and tear. The simultaneity and geographic spread of the damage pointed firmly toward physical sabotage or a coordinated attack.

Shortly after these findings emerged, a group calling itself Specter publicly claimed responsibility. The group described itself as independent of any state, but well-funded and in possession of advanced marine engineering knowledge. Its stated motivations remain unclear. The committee convenes at this point: the damage is confirmed, the claim of responsibility has been received, and the international community is watching for a response.

6.2 Precedents and Illustrative Case Studies

The Specter scenario is fictional, but it is built around a pattern of vulnerability that real events have already established. Two cases are particularly relevant.

6.2.1 Tonga, 2022

On 15 January 2022, the Hunga Tonga–Hunga Ha'apai underwater volcanic eruption damaged the 827-kilometre submarine cable connecting Tonga to Fiji — the country's only international fibre-optic link. The result was near-total isolation from global internet connectivity. Repair operations required 20 days of cable ship work, and the country went without reliable international connectivity for more than five weeks overall.

Tonga is the clearest real-world case of single-point national dependency. When one cable is the only connection and it is severed, the consequences are severe and the recovery is slow. The case also illustrates the logistical reality of deep-sea cable repair: deploying the right

vessel, obtaining permits, navigating difficult sea conditions, and physically locating and fixing the fault all consume significant time — time during which a country remains cut off.

6.2.2 The Baltic Sea, 2025–2026

The Baltic Sea incidents present a different kind of challenge. In January 2025, damage to a fibre-optic cable between Latvia and Sweden triggered a formal sabotage investigation and NATO patrol deployment — part of a broader pattern of incidents affecting cable and energy infrastructure in the region. In response, Finland announced in January 2026 plans for a maritime surveillance centre equipped with seabed sensors, vessel-information exchange systems, and real-time analysis tools specifically designed to protect undersea infrastructure. NATO's Baltic Sentry programme was launched around the same time for the same purpose.

Unlike Tonga, the significance of the Baltic cases lies not primarily in the disruption caused, but in what they reveal about how states are beginning to think about cable security. The shift — from treating cable incidents as maintenance events to treating them as potential acts of aggression requiring military surveillance and legal investigation — is directly relevant to the attribution and response challenges this committee will face.

7. Legal and Coordination Framework

7.1 The United Nations Convention on the Law of the Sea

The primary legal framework governing submarine cables and the seas in which they are laid is the United Nations Convention on the Law of the Sea — UNCLOS. Several of its provisions bear directly on this committee's agenda.

Article 79 addresses the right to lay cables and pipelines on the continental shelf. Article 112 establishes the same right for the bed of the high seas, beyond any state's continental shelf. Together, these articles set the basic legal foundation for the existence of international submarine cable infrastructure. Most significantly, Article 113 requires all states parties to adopt domestic laws making the deliberate breaking or injury of a submarine cable a punishable criminal offence. This is the legal basis for any criminal accountability tied to intentional cable damage. However, enforcement depends entirely on national implementation — UNCLOS creates no international enforcement mechanism, and no international court holds automatic jurisdiction over cable damage incidents.

7.2 The 1884 Convention for the Protection of Submarine Telegraph Cables

The 1884 Convention for the Protection of Submarine Telegraph Cables is one of the oldest international agreements still relevant to cable infrastructure, and its age does not diminish its legal force. It applies outside territorial waters to established submarine cables, protects repair operations, and requires other vessels to maintain a safe distance from ships engaged in cable repair work. States parties are obligated to prosecute violations and to cooperate in preventing interference with cable operations.

One provision within the Convention's explanatory declaration is particularly relevant to this committee: penal responsibility does not apply to accidental breakage where all reasonable precautions were taken. This creates an explicit legal distinction between deliberate damage and unavoidable accident — a distinction that sits at the heart of every attribution question delegates will face.

7.3 The Tampere Convention

The Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations establishes a legal framework for cross-border sharing of telecommunications assistance during disasters and emergencies. It defines such assistance broadly, allows affected states to formally request it from other states and international

organizations, and requires states parties to reduce or remove — wherever possible and consistent with national law — the regulatory barriers that might otherwise delay the flow of assistance.

Those barriers can include restrictions on the import of equipment, limitations on the movement of personnel, spectrum licensing requirements, and transit delays. For this committee, the Tampere Convention functions as a legal tool that can be invoked to justify the rapid cross-border sharing of equipment, personnel, and communications capacity during an active crisis.

7.4 Regulatory Bottlenecks and Practical Constraints

The most serious practical obstacle to fast cable repair is not the physical difficulty of the work — it is the regulatory friction that prevents repair vessels from reaching the fault in time. The ITU's 2025 reporting explicitly identifies permitting procedures, customs requirements, and cabotage laws as major causes of prolonged outages.

Cabotage laws are domestic regulations that restrict or prohibit foreign vessels from operating in a country's territorial waters. Because specialist repair ships are rare, the closest available vessel at the time of a fault is often registered in a foreign country. If cabotage rules prevent that vessel from entering national waters, it cannot perform the repair — regardless of the emergency. Customs requirements for the temporary import of specialist equipment, and the need for environmental and maritime permits before repair work begins, can each add days or weeks to the response timeline.

The Porto Declaration of February 2026, discussed in Section 8, responds directly to these bottlenecks — calling for single government contact points, more transparent repair procedures, and reduced barriers in customs, cabotage, and marine spatial planning.

7.5 ITU's Institutional Role Within This Framework

The ITU's role within this legal landscape is institutional and coordinative rather than coercive. It cannot order states to act, enforce international law, or deploy enforcement assets. What it can do is facilitate dialogue, develop common standards, provide technical expertise, and bring together the full range of stakeholders — governments, private operators, technical bodies, and international organizations — whose cooperation any effective response requires.

The ITU is now directly engaged in submarine cable resilience through the International Advisory Body for Submarine Cable Resilience, established jointly with the ICPC in November 2024. This body is the most important current platform for practical multilateral

cooperation on cable infrastructure, and it provides the direct institutional context within which this committee operates.

8. Prior Actions and Existing Mechanisms

8.1 The ITU-ICPC International Advisory Body for Submarine Cable Resilience

The International Advisory Body for Submarine Cable Resilience was established jointly by the ITU and the International Cable Protection Committee in November 2024. Its stated purpose is to promote dialogue and collaboration aimed at improving the resilience of the infrastructure that powers global communications and the digital economy.

The body brings together member states, cable operators, technology companies, and technical experts in a structured format built to produce practical recommendations rather than political declarations alone. Its creation reflects a recognition — now shared across governments and industry — that the governance gap around submarine cable infrastructure had become untenable, and that a dedicated multilateral mechanism was needed to address it seriously. For delegates, this body is the direct institutional parent of this committee's mandate; its Working Group 2 recommendations, produced in February 2026, provide a technically grounded framework of policy options that the committee can draw upon, develop, or adapt in its directives.

8.2 The Abuja Summit and the Porto Declaration

Two major international gatherings in 2025 and 2026 have advanced the policy agenda on submarine cable resilience.

The Abuja Summit of 2025 confirmed that the world's undersea cable network constitutes critical global infrastructure, emphasizing the need for stronger international cooperation, more diverse cable routes and landing points, and timely repair and deployment. It served as a high-level political affirmation of the issue's importance.

The Porto Declaration of February 2026 went further, endorsing concrete non-binding guidance. Its key commitments include streamlined regulatory procedures for cable repair, reduced legal and administrative barriers in customs and cabotage, investment in route diversity and redundant landing points, stronger public-private partnerships, and targeted support for the most vulnerable states. The Declaration does not create binding obligations, but it represents the most recent and detailed international consensus on what practical measures should be taken — and it was adopted just weeks before the crisis this committee is convening to address.

8.3 Emergency Response Tools and Regional Security Developments

On the emergency response side, the ITU already operates tools directly relevant to the current crisis. The Disaster Connectivity Map provides real-time information on connectivity disruptions and had been activated in more than 80 countries and disaster events as of January 2026. The ITU also supports national emergency telecommunications planning and provides implementation assistance tied to the Tampere Convention's framework for cross-border telecommunications assistance.

On the security side, developments in the Baltic region show how some parts of the world have already moved beyond purely reactive repair logic toward continuous monitoring and deterrence. NATO's Baltic Sentry programme and Finland's planned maritime surveillance centre — with seabed sensors and vessel-tracking systems — represent an emerging model of proactive infrastructure protection that delegates may wish to draw on when drafting the committee's response.

9. Key Stakeholders and Relevant Actors

An effective committee response depends not only on understanding the technical and legal dimensions of the crisis, but on understanding the full range of actors whose cooperation — or resistance — will shape any real-world outcome.

Member States and National Regulators. Governments control domestic licensing, security regulations, customs procedures, port access, environmental permitting, marine spatial planning, and the national implementation of international legal obligations such as UNCLOS Article 113. No international response works without state-level action, and the speed and quality of each state's response will vary considerably depending on its regulatory environment and the degree to which it has invested in preparedness.

The ITU and the ICPC. The ITU provides the multilateral forum for coordination and standard-setting; the ICPC provides concentrated industry expertise on cable operations, repair practices, and protection standards. Together, through the joint Advisory Body, they form the most important current platform for international action on cable resilience.

Cable Owners, Operators, and Consortia. These private entities control the physical infrastructure, including the operational data, maintenance protocols, and repair interfaces

that any response requires. Because cables are generally built, owned, and operated by private actors, their active participation is not optional — it is indispensable.

Hyperscalers, Cloud Firms, IXPs, and Data Centre Operators. Large technology companies increasingly shape global traffic flows and resilience outcomes through investment decisions, hosting practices, content caching, and network peering arrangements. IXP operators and local data centre providers directly affect how resilient national connectivity is when international cables are disrupted — as the Bangladesh case showed clearly.

Maritime and Enforcement Actors. Port authorities, coast guards, navies, customs agencies, and law-enforcement bodies become central actors in any scenario involving suspected sabotage, vessel tracking, repair logistics, or the investigation of a third-party attack. The Working Group 2 recommendations call explicitly for stronger cooperation with law-enforcement agencies, enhanced enforcement of vessel-tracking systems, and port-state inspection of anchors in sensitive areas.

10. Key Issues, Delegate Questions, and Proposed Solutions

10.1 Key Issues Before the Committee

Five interconnected issues define the core challenges the committee must address.

The first is **attribution**. Distinguishing between accidental damage, negligence, and deliberate sabotage is technically and legally difficult, particularly when the physical method — anchor dragging, for instance — looks the same in all three cases. The 1884 Convention draws an explicit legal distinction between intentional damage and unavoidable accident, but real-world evidence rarely arrives quickly or neatly. The Baltic Sea incidents show how suspicion can develop long before proof is established, and how investigation and surveillance mechanisms currently struggle to keep pace.

The second is **repair speed**. Even when a fault is physically located, restoring connectivity can be delayed for weeks by permitting procedures, customs requirements, cabotage restrictions, and the logistical challenge of deploying specialist vessels to remote locations. Tonga's more than five weeks without reliable international connectivity is the clearest

illustration of what is at stake. These delays are largely regulatory and administrative in nature — not technical.

The third is **resilience design**. The severity of a cable disruption's impact on a given country depends heavily on decisions made before the disruption occurs: whether multiple cable routes exist, whether landing points are diverse, whether significant content is hosted locally, whether IXPs are strong, and whether satellite fallback is available. Bangladesh and Tonga sit at opposite ends of this spectrum. Building baseline resilience across all countries — not just responding to individual crises after they occur — is a strategic priority.

The fourth is **public-private coordination**. States hold the political and legal responsibility for public safety and infrastructure protection, but they do not own or directly control most of the infrastructure at stake. Bridging this structural gap between public responsibility and private ownership is essential both for responding to the current crisis and for building a more durable governance framework going forward.

The fifth is **inequality of exposure**. Small island developing states, least developed countries, landlocked developing countries, and underserved regions face disproportionately severe consequences from cable disruptions — fewer cables, less route diversity, weaker local hosting, and fewer resources for rapid response. A solution that does not address this inequality will leave the most vulnerable populations the least protected.

10.2 Questions Delegates Should Consider

The following questions are intended to guide delegate preparation and focus the committee's deliberations:

- What level and type of evidence should be required before a multilateral body formally attributes cable damage to sabotage rather than accident? How should the committee act before attribution is confirmed?
- How can states accelerate cable repair without compromising their sovereignty over customs procedures, cabotage regulations, and maritime permitting?
- What minimum standards of resilience — in terms of route diversity, landing diversity, local hosting, and emergency backup — should apply to all countries connected to global infrastructure?
- How should responsibility be divided among governments, private cable operators, cloud firms, and technical bodies during a multi-cable emergency?

- What specific forms of support should be prioritized for small island states, least developed countries, and other highly exposed nations with limited international connections?

10.3 Proposed Solutions and Policy Approaches

The Porto Declaration and the Working Group 2 recommendations together point toward six major policy directions delegates should consider when drafting directives.

Single-window repair coordination. Each country should designate a single government contact point for cable repair, with clear and transparent procedures so that repair vessel operators know exactly what permissions are required, from whom, and how quickly a response can be expected.

Legal and regulatory streamlining. Customs barriers, cabotage restrictions, and marine planning delays should be reduced through pre-negotiated arrangements or emergency exemption procedures that allow repair assets to be deployed without unnecessary administrative delay.

Resilience by design. Policy frameworks should actively encourage route diversity, redundant landing points, security hardening of cable stations, maintenance of spare cable stock, and regular stress testing of the network — not only after a disruption, but as a continuous and routine practice.

Improved information sharing. Standard reporting protocols, shared threat assessments, and structured cooperation between governments and private operators can reduce the information gaps that currently complicate both real-time crisis response and long-term planning.

Enhanced enforcement. Stronger domestic implementation of the cable-damage criminal offences required by UNCLOS Article 113, combined with better enforcement of vessel-tracking systems and inspection of anchors in cable-sensitive zones, can improve deterrence and accountability.

Special support for vulnerable states. Targeted partnerships, capacity-building programmes, resilience investment, and technical assistance for small island developing states, least developed countries, and other underserved regions should be embedded in any durable international framework — not added as an afterthought once the immediate crisis is resolved.

11. Expectations and Closing Remarks

The scenario this committee addresses is fictional, but it is grounded in challenges that are real, ongoing, and rapidly growing in strategic importance. The events of the past two years — from the Baltic Sea investigations to the Porto Declaration — show that the international community is only beginning to build the legal, institutional, and technical frameworks needed to protect critical undersea infrastructure. This committee meets at precisely that moment of transition.

Delegates should come to proceedings with three priorities in mind:

- The first is practical action. Directives will be assessed not only on how ambitious they are, but on how realistic and implementable they are. Responses that are specific, technically grounded, and operationally coherent carry far more weight than vague political statements.

- The second is breadth of stakeholder thinking. No effective response to this crisis will come from governments alone, or from the private sector alone, or from the ITU alone. Solutions that matter require simultaneous coordination across all of these actors.

- The third is taking inequality of exposure seriously. A response that restores connectivity for major economies while leaving small island states and least developed countries isolated is not a complete solution. The committee's directives should reflect the understanding that resilience must be built for everyone — not only for those who already have the most.

The committee leadership looks forward to seeing how delegates engage with one of the defining infrastructure security challenges of the twenty-first century.

Appendix A: Key Terms and Concepts

Submarine cable: A fibre-optic cable laid on or under the seabed to carry international communications and data.

Cable landing station (CLS): A shore-based facility where an international submarine cable terminates and connects to national terrestrial networks.

First mile: The international connectivity layer through which the internet enters a country, including submarine cables, landing stations, satellite links, and cross-border systems.

Middle mile: The national backbone layer carrying traffic across a country through long-distance fibre, internet exchange points, local hosting, and related infrastructure.

IXP (Internet Exchange Point): A physical location where different networks connect and exchange data traffic, keeping local traffic local and improving resilience.

Route diversity: The availability of varied cable routes and landing points so that traffic can shift away from a damaged corridor.

Chokepoint risk / clustered landing risk: Vulnerability created when many cable systems converge on the same geographic location or route corridor, so a single incident affects multiple cables at once.

AIS (Automatic Identification System): A vessel-tracking system transmitting the location, speed, and identity of ships; relevant to identifying suspect vessel movements near cable incidents.

Cabotage: Domestic shipping regulations restricting or prohibiting foreign vessels from operating in a state's territorial waters; a significant source of delay in cable repair operations.

Attribution: The process of determining who or what caused cable damage and whether the cause was accidental, negligent, or intentional.

Resilience: The capacity of a telecommunications system to withstand, respond to, and recover from disruption.

Wet plant: The submerged components of a submarine cable system, including the cable, repeaters, and branching units.

Dry plant: The shore-based components of a submarine cable system, including transponders, power-feed equipment, and monitoring systems at landing stations.

Bibliography

"About The International Telecommunication Union (ITU)." International Telecommunication Union, accessed 21 Mar. 2026.

"Building Resilient National ICT Infrastructure in Asia and the Pacific." International Telecommunication Union, 2025.

"Convention for the Protection of Submarine Telegraph Cables (Paris, 14 March 1884)." International Cable Protection Committee, accessed 21 Mar. 2026.

"Disaster Connectivity Map." International Telecommunication Union, accessed 21 Mar. 2026.

"Emergency Telecommunications." International Telecommunication Union, accessed 21 Mar. 2026.

"Finland Hopes to Prevent Cable Damage with New Surveillance Centre." Reuters, 26 Jan. 2026.

"Global Connectivity Report 2025." International Telecommunication Union, 2025.

"International Advisory Body for Submarine Cable Resilience." International Telecommunication Union, accessed 21 Mar. 2026.

"International Summit Outlines Steps to Improve Resilience of Submarine Telecommunications Cables Worldwide." International Telecommunication Union, 27 Feb. 2025.

"The Impact of Natural Disasters on Telecom Subsea Cable Systems." International Telecommunication Union Workshop Material, 2024.

"The January 15, 2022 Hunga Tonga–Hunga Ha'apai Eruption." World Bank, 2022.

"Overview of ITU's History." International Telecommunication Union, accessed 21 Mar. 2026.

"Porto Declaration on Submarine Cable Resilience." International Telecommunication Union, 3 Feb. 2026.

"Risk Identification, Monitoring and Mitigation: Working Group 2 Recommendations." International Telecommunication Union, Feb. 2026.

"Sweden Opens Sabotage Probe into Baltic Undersea Cable Damage." Reuters, 26 Jan. 2025.

"Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations." United Nations Treaty Series, 18 June 1998.

"United Nations Convention on the Law of the Sea." United Nations, 1982.

"Written Testimony on Submarine Cables." TeleGeography, 2025.