INTERNATIONAL TELECOMMUNICATIONS UNION

13-15th of March, 2026

TOPIC: SECURING GLOBAL INFRASTRUCTURE AND UNDERSEA CABLES IN TIMES OF CRISIS

Sponsors: Japan, Singapore, South Korea.

Signatories: Canada, People´s Republic of China, Federal Republic of Germany, France, Islamic Republic of Iran, Kingdom of the Netherlands, Republic of China (Taiwan), United States of America, United Kingdom of Great Britain.

Preambulatory clauses:

Recalling its mandate under the International Telecommunications Union Constitution and Convention to coordinate global telecommunications and set technical standards,

Recognizing that undersea cables carry approximately 95 to 99 percent of all transoceanic digital communications, making them indispensable for global economic stability and national security,

Deeply concerned by the vulnerability of this infrastructure to accidental damage, natural disasters, and hybrid threats such as state-sponsored sabotage and espionage,

Guided by the principles of the United Nations Convention on the Law of the Sea (UNCLOS), particularly Articles 113-115 regarding the protection of submarine cables;

Operative clauses:

FUNDING AND OVERSIGHT FRAMEWORK

1. *Encourage the establishment* of a Global Infrastructure Resilience Fund (GIRF) as a targeted emergency contingency fund to preserve global communication stability;

2. *Suggest* that national contributions to said fund be determined by a Weighted Responsibility Index calculated using three primary metrics:

   a. GDP per capita to ensure economic capability,
   b. Size of the population to account for digital demand,
   c. Real use of infrastructure is measured by international bandwidth traffic volume.

3. Further recommends that the fund shall be managed by the ITU Telecommunication Development Bureau (BDT), utilizing its existing frameworks for technical assistance and infrastructure partnership;

CRISIS RESPONSE AND SUBSTITUTION INFRASTRUCTURE

4. Endorses the development of Alternative Substitution Infrastructure (ASI) to preserve primary communication systems during cable outages with the critical funds previously mentioned, specifically prioritizing:

a. Satellite bridging to be coordinated through ITU regulations,
b. Route diversification to reduce systemic risk in high-traffic corridors;

5. Calls for the maintenance of a geographical map of high-risk zones, specifically targeting corridors such as the Northern Sea, Malacca Strait, and Red Sea, where cable concentration and the geopolitical context increase vulnerability to assist protection for;

a. Cable concentration in these regions, combined with volatile geopolitical contexts, increases systemic vulnerability to global connectivity;
b. The mapping initiative shall serve as the primary diagnostic tool to prioritize the allocation of resources from the Global International Resilience Fund (GIRF) to areas of highest impact;
c. The deployment of Alternative Substitution Infrastructure (ASI) to ensure nations within these corridors maintain primary communication systems during disruptions;
d. International coordination to protect these "digital chokepoints," supporting the deployment of specialized repair hubs and security monitoring where it is most critical;

EMPOWERMENT AND TECHNICAL INDEPENDENCE

6. Understands the importance of the creation of a bank of knowledge as a centralized ITU repository for technical data, repair protocols, and environmental sensing technology:

a. *Mandating* that this platform provides training initiatives to help developing nations manage their own landing stations independently, reducing reliance on foreign-owned infrastructure;

7. Encourages a Public-Private framework that distinguishes risk sectors and standardizes security based on priority matters, while encouraging private innovation through mixed investment;

SECURITY AND PRIVACY

8. Urges all member states to legislate toward the recognition of cable sabotage as an international threat;

9. Supports the implementation of AI-driven threat detection to identify traffic anomalies and provide real-time alerts to national cybersecurity centers regarding potential physical or cyber-threats;

10. Standardizes safety measures to preserve hardware systems, specifically at landing stations, through mandatory hardware transparency and secure encryption standards to protect user privacy.

"Technology is our strength, and we use it to protect our information"