

The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World

Communications networks underpin almost every aspect of our lives. Yet the rapid development of communication technologies and massive scale of these networks increases our dependency on these systems and introduces vulnerabilities.

Undersea cables, together with other elements of the information and communications technology ecosystem, continue to transform the way we communicate and the way we live. The unparalleled capacity, low latency, and reliability of undersea cables make them ideal for transmitting vast volumes of data and information. The demand for undersea cables and supporting infrastructure has surged as seamless connectivity has become indispensable to commerce and digital growth across every sector of the global economy. The expansion of undersea cable networks is the foundation of a more interconnected and interdependent global community, and states should adopt policies to enable efficient, robust, redundant, resilient, and secure infrastructure for network data and information flows.

This reliance on undersea cables can, however, present major risks related to important public interests and have national and economic security implications. Protecting the security, resilience, and integrity of undersea cables is critical to global communications, economic growth, and development. Managing security risks, including from high-risk suppliers of undersea cable equipment and promoting best security practices for laying and maintaining these cables for secure and resilient global infrastructure is essential for the networks upon which the global economy relies.

In this regard, undersea cable infrastructure includes not only the communication cables themselves but also any elements related to their construction, operation, surveillance, maintenance and repair, such as landing stations, software, and the terrestrial parts of the submarine cable connecting to them, repair centers, as well as the fleet of deployment, maintenance and repair vessels.

The endorsers aspire to the following principles for a shared global approach to ensure the security, reliability, interoperability, sustainability, and resiliency for the deployment, repair and maintenance of undersea cable infrastructure:

- Design undersea cable infrastructure and services with resilience, redundancy, and security in mind. Build and maintain this infrastructure incorporating cybersecurity best practices that safely facilitate international communication.

- Advance cooperation between endorsers to promote the selection of secure and verifiable subsea cable providers for new cable projects, in particular for intercontinental ICT cable projects, reduce latency and enhance route diversity, protect cables and anticipate risks of intentional or unintentional damage as well as risks of communications and data being compromised.
- Seek closer government and industry coordination for supporting responsible undersea cable deployment, maintenance, and repair according to established international industry norms.
- Emphasize the importance of spatial and route planning to promote coordinated use of seabeds, protect cables from natural or man-made hazards, ease chokepoints, and reduce risk of inadvertent disruption while expanding global connectivity. Encourage where applicable alternative submarine cable routes in view to improve resilience of the global cables network.
- Share with interested third parties and governments best practices for permitting and regulation to support international cable systems and supporting services and capabilities.
- Encourage undersea cable network service providers and operations and maintenance providers to have transparent ownership, partnerships, and corporate governance structures.
- Consider security risk assessments regularly across the cable lifecycle, taking into account technical and non-technical risk factors such as undue influence by a third country on suppliers and service providers, while developing and implementing risk mitigation measures.
- Promote data risk mitigation frameworks and data security measures to protect cable networks from unauthorized access to data in transit or storage for dual purposes.
- Comply with applicable international law, as reflected in UNCLOS, and domestic law and consider relevant policies at regional or national level, as well as applicable industry best practices, notably with regard to risk assessment and management.

By endorsing these principles, we hope other nations will follow these principles within their respective systems of government and thereby create collaborative action to better preserve the reliability, integrity, security, and availability of infrastructure that supports the global community.