International Cable Protection Committee

Law of the Sea Workshop

2024

SINGAPORE

Dean Veverka

Sharing the seabed and oceans in harmony

Security of Submarine Cables

- Security of submarine cables is critical to ensure reliability and resilience of the world’s communication super highway.

- Greater Governmental awareness of the complex interdependencies of other industry sectors on submarine cables.

- Importance of and recognition that Submarine Cables are critical Infrastructure for most countries.

What are the threats

- Threats can be physical or cyber initiated
- Physical include – fishing, anchoring, seismic, malicious, sabotage
- Cyber include – corruption of user data, loss of control of Network Management Systems

Security Limitations

- Cables cannot be hidden, buried or armored sufficiently to avoid malicious attacks, or guarded along their entire routes
- Declining to chart cables is not an option, as it would exacerbate fishing and anchoring damage, undermine ability of operators to pursue damages claims, and arguably fail to show due regard for other marine activities although operators may decide not to chart in close proximity to shore in order to minimize targeting of landing facilities
- Absence of international consensus prohibiting attacks on cables by states during peacetime, wartime, and circumstances in between remains problematic
    - UNCLOS is silent on security and malicious attacks
    - 1884 Convention creates exemption for attacking cables in wartime

Solutions

- Cable operators and suppliers can and should adopt physical and logical security policies, supply chain security measures, personnel screening, and resilience strategies to secure infrastructure and secure communications over than infrastructure.
- Ultimately, however, states have the best intelligence regarding state and many non-state threats to cables—and the ability to deter or respond to state actions against cables.
- Governments and operators should share information in both directions to identify and mitigate risks
- Governments should be cognizant of their own actions and policies (e.g., policies that encourage clustering of routes and landings and impair geographic diversity and permitting policies that delay repairs) that can harm network resilience and magnify the impact of malicious attacks

Best Practice Guidelines

Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables

- Focus on statistically-significant risks where government action could have the greatest impact on risk reduction;
- Observe and implement treaty obligations (particularly under the United Nations Convention on the Law of the Sea ("UNCLOS")) and customary international law defining state jurisdiction over, and protection of, submarine cables eg
- Spatial Separation
- Nautical Charting
- Marine Spatial Planning
- Single Point of Contact
- Route and Landing Optimisation, Geographic Diversity
- Permitting for Installation and Repair
- Cabotage and crewing restrictions
- Critical Infrastructure designation; eg Australia's legislation "Security of Critical Infrastructure (SOCI) Act (2018)".

Thank you.

International Cable Protection Committee

Law of the Sea Workshop

2024

SINGAPORE

Dean Veverka

Sharing the seabed and oceans in harmony