1. Digital Chokepoints in The Era of Global Connectivity – International Relations

Amid rising geopolitical tensions, Undersea Cable Networks passing through strategic Digital Chokepoints have emerged as highly vulnerable infrastructure.

1.Background

The modern digital economy depends fundamentally on seamless global connectivity enabling instantaneous communication, financial transactions, cloud computing, streaming services, and data exchange across continents. This connectivity relies overwhelmingly on undersea or submarine cables—fibre-optic communication cables laid on the seabed to transmit internet and telecommunication data across countries and continents—rather than satellites which many mistakenly believe carry majority of international internet traffic. More than 500 submarine cables connect different parts of the world, and around 95% of global internet and international data traffic passes through these cables making them absolutely critical infrastructure for global economy. Undersea cables support global banking systems processing trillions of dollars in daily transactions, digital payments enabling e-commerce and remittances, cloud computing services hosting data and applications for businesses and governments, and military communications ensuring command-and-control capabilities.

Major technology companies such as Google, Meta, and Microsoft are increasingly investing in submarine cable infrastructure recognizing strategic importance for their global operations. However, these cables face significant vulnerabilities particularly where they pass through narrow maritime passages called digital chokepoints—narrow maritime passages through which multiple submarine communication cables pass together creating concentration risks. These chokepoints become strategically important because disruption at one location can affect internet connectivity across several regions simultaneously. Major global digital chokepoints include Strait of Hormuz serving as major digital and energy chokepoint connecting Gulf region with global economy, Bab El-Mandeb Strait linking Red Sea with Arabian Sea carrying major submarine cable routes, Suez Canal acting as crucial corridor connecting Europe and Asia through both maritime trade and digital infrastructure, Malacca Strait connecting Indian Ocean with Pacific Ocean carrying vital communication networks, and Red Sea hosting several critical undersea cable systems connecting Europe, Asia, and Africa. Rising geopolitical tensions particularly in West Asia involving conflicts, military operations, and strategic competition have exposed vulnerability of submarine cables to intentional sabotage, accidental damage from anchors and fishing equipment, natural disasters including earthquakes and underwater landslides, and aging infrastructure requiring maintenance and upgrades.

The emergence of infrastructure geopolitics where digital infrastructure is increasingly becoming an instrument of geopolitical influence and strategic leverage, rise of hybrid warfare where states may use cyberattacks, sabotage, or infrastructure disruption below threshold of conventional warfare to pressure rival countries, and growing maritime competition with seabed emerging as new domain of strategic competition involving countries such as United States, China, Russia, and Iran create unprecedented security challenges for undersea cable networks requiring coordinated international responses, enhanced maritime surveillance, redundant infrastructure, and stronger legal frameworks protecting critical digital infrastructure.

2.Undersea Cables - Foundation of Global Connectivity

Key Features

1. More than 500 submarine cables connect different parts of the world creating global digital network spanning hundreds of thousands of kilometres.
2. Around 95% of global internet and international data traffic passes through these cables demonstrating overwhelming dependence on this infrastructure.

3. Undersea cables support global banking systems processing daily transactions worth trillions of dollars, digital payments enabling e-commerce worth billions annually, cloud computing services hosting critical data and applications for businesses and governments, and military communications ensuring command-and-control capabilities during peace and conflict.
4. Major technology companies such as Google, Meta, and Microsoft are increasingly investing in submarine cable infrastructure recognizing strategic importance for global operations and competitive advantage.

Technical Characteristics

1. Submarine cables use fibre-optic technology transmitting data as pulses of light enabling high-speed, high-capacity transmission.
2. Cables are typically buried in shallow waters near shores for protection but lie exposed on deep ocean floors.
3. Modern cables can transmit terabits of data per second sufficient for millions of simultaneous video calls or data transfers.
4. Cable systems include landing stations on shore where submarine cables connect to terrestrial networks and power feeding equipment provides electrical power.

Digital Chokepoints - Strategic Vulnerabilities

Definition and Significance

1. Digital chokepoints are narrow maritime passages through which multiple submarine communication cables pass together creating concentration of critical infrastructure.
2. These chokepoints become strategically important because disruption at one location can affect internet connectivity across several regions simultaneously.
3. Concentration of cables in few locations creates dangerous single points of failure where one incident can cascade across multiple networks.

Major Global Digital Chokepoints

Strait of Hormuz - Serves as a major digital and energy chokepoint connecting the Gulf region with the global economy, carrying cables linking Europe, Middle East, and Asia while also transporting significant portion of global oil and gas supplies creating dual strategic importance.

Bab El-Mandeb Strait - Links the Red Sea with the Arabian Sea and carries major submarine cable routes connecting Europe with Asia and Africa, with recent Houthi attacks in region highlighting vulnerability.

Suez Canal - Acts as a crucial corridor connecting Europe and Asia through both maritime trade and digital infrastructure, with ever-increasing data traffic passing through cables in region.

Malacca Strait - Connects the Indian Ocean with the Pacific Ocean and carries vital communication networks linking major Asian economies with rest of world.

Red Sea - Hosts several critical undersea cable systems connecting Europe, Asia, and Africa, with geopolitical instability in region creating persistent vulnerability.

3.Geopolitical Dimensions of Undersea Cables

Emergence of Infrastructure Geopolitics

1. Digital infrastructure is increasingly becoming an instrument of geopolitical influence and strategic leverage as nations recognize control over connectivity infrastructure provides power.
2. Countries compete for influence over cable routes, landing stations, and maintenance capabilities creating new dimension of great power competition.
3. Infrastructure investment is being used as tool of diplomacy and influence particularly by China through Digital Silk Road initiatives.

Rise of Hybrid Warfare

1. States may use cyberattacks, sabotage, or infrastructure disruption below the threshold of conventional warfare to pressure rival countries.

2. Hybrid tactics allow plausible deniability while achieving strategic objectives without triggering full-scale conflict.
3. Disruption of submarine cables can create economic pressure, information blackouts, and political instability in target countries.

Growing Maritime Competition

1. The seabed is emerging as a new domain of strategic competition involving countries such as the United States, China, Russia, and Iran.
2. Naval capabilities for underwater surveillance, cable monitoring, and rapid repair are becoming important elements of maritime power.
3. Competition extends to seabed mapping, deep-sea technology, and control of strategic underwater terrain.

4.Major Vulnerabilities

Concentration of Infrastructure

1. Many submarine cables are concentrated along the same seabed routes, creating dangerous single points of failure where one incident affects multiple systems.
2. Economic efficiency considerations drive cable clustering along proven routes rather than geographic diversification.
3. Landing stations where multiple cables converge create additional concentration vulnerabilities.

Difficulty in Repair Operations

1. Repairing damaged submarine cables requires specialised ships with cable-laying capabilities, technical expertise in splicing fibre-optic cables underwater, and international coordination for access to territorial waters and exclusive economic zones.
2. Repair operations become difficult during military tensions or maritime conflicts when access to damaged cable locations may be restricted.
3. Average repair time ranges from days to weeks depending on location, weather conditions, and availability of repair ships.

Legal and Regulatory Ambiguity

1. International legal frameworks regarding intentional cable disruption remain weak and ambiguous, especially in situations involving hybrid warfare or grey-zone conflicts.
2. United Nations Convention on the Law of the Sea provides some protection but enforcement mechanisms are limited.
3. Attribution of responsibility for cable damage is often difficult particularly when sabotage is suspected.

5.Potential Consequences of Cable Disruption

Disruption of Global Connectivity

1. Damage to submarine cables can reduce internet speed affecting business operations and consumer services, disrupt communication networks isolating regions from global information flows, and create regional internet blackouts paralyzing economic and social activities.

Financial Instability

1. Interruptions in data flows can affect banking systems disrupting transactions and settlements, impact stock markets creating volatility and trading disruptions, compromise global payment networks affecting commerce, and increase economic uncertainty affecting investment and growth.

Impact on Global Trade

1. Digital disruptions can affect shipping operations relying on real-time data and communication, disrupt insurance markets requiring connectivity for underwriting and claims, impact supply chains dependent on just-in-time coordination, and affect energy trade routes particularly in Gulf region.

Security and Military Risks

1. Damage to submarine cables can weaken military coordination across theatres of operation, disrupt intelligence communication affecting national security, and compromise command-and-control systems during crises when reliability is most critical.

Disproportionate Impact on Developing Countries

1. Developing countries with limited digital backup infrastructure may face severe communication and economic disruptions creating longer recovery times and greater economic losses compared to developed nations with redundant systems.

6.Concerns for India

Economic Dependence

1. India's financial and IT sectors are highly dependent on uninterrupted data connectivity for global operations.
2. IT services exports worth over $200 billion annually require reliable international connectivity.
3. Financial sector processes billions of dollars in daily transactions through submarine cable networks.

Geopolitical Risks

1. Rising geopolitical tensions in the Indian Ocean Region increase risks to digital infrastructure passing through regional chokepoints.
2. India's cables pass through Bab el-Mandeb Strait, Red Sea, Strait of Hormuz, and Malacca Strait—all facing elevated security risks.

Strategic Vulnerabilities

1. Dependence on foreign-controlled cable infrastructure creates strategic vulnerabilities where external actors could influence India's connectivity.
2. Limited domestic capabilities in cable manufacturing, laying, and repair create dependence on foreign companies.

7.Way Forward

Diversification of Cable Routes

1. Countries should develop alternative submarine cable routes to reduce excessive dependence on a few chokepoints, exploring Arctic routes, trans-Pacific alternatives, and Africa circumnavigation options, while investing in redundant cable systems ensuring connectivity even when primary routes are disrupted.

Strengthening Maritime Security

1. Naval cooperation and maritime surveillance should be enhanced to protect underwater digital infrastructure through joint patrols in critical areas, information sharing on suspicious activities, and rapid response capabilities for cable protection.

Building Redundant Systems

1. Countries should invest in satellite communication systems and backup digital infrastructure to improve resilience, developing hybrid networks combining submarine cables with satellite links, while maintaining strategic data centers domestically reducing dependence on international connectivity for critical functions.

International Cooperation

1. Global cooperation is required for protection of submarine cables through multilateral frameworks, faster repair coordination enabling rapid response to cable damage, information sharing on threats and incidents, and development of legal norms regarding infrastructure protection establishing clear consequences for intentional disruption.

Indigenous Capabilities

1. India should develop domestic capabilities in cable manufacturing reducing import dependence, cable-laying operations through specialized vessels, and maintenance and repair through training programs and infrastructure investment, while encouraging private sector participation through policy support and incentives.

Conclusion

Undersea cable networks carrying 95% of global internet and international data traffic through more than 500 submarine cables have emerged as highly vulnerable infrastructure amid rising geopolitical tensions. Digital chokepoints including Strait of Hormuz, Bab El-Mandeb Strait, Suez Canal, Malacca Strait, and Red Sea where multiple submarine communication cables pass together create concentration risks where disruption at one location affects connectivity across several regions simultaneously. Geopolitical dimensions include emergence of infrastructure geopolitics using digital infrastructure as instrument of influence, rise of hybrid warfare employing sabotage below conventional warfare threshold, and growing maritime competition with seabed as new domain involving United States, China, Russia, and Iran.

Major vulnerabilities include concentration of infrastructure along same routes creating single points of failure, difficulty in repair operations requiring specialized ships and international coordination, and legal and regulatory ambiguity regarding intentional disruption. Potential consequences include disruption of global connectivity, financial instability affecting banking and payment systems, impact on global trade, security and military risks, and disproportionate impact on developing countries. For India, concerns include dependence of financial and IT sectors on uninterrupted connectivity, rising geopolitical tensions in Indian Ocean Region, and dependence on foreign-controlled infrastructure. Addressing vulnerabilities requires diversification of cable routes reducing chokepoint dependence, strengthening maritime security through naval cooperation and surveillance, building redundant systems including satellite communication, international cooperation for cable protection and legal norms, and developing indigenous capabilities in manufacturing, laying, and maintenance.
Source -https -//www.downtoearth.org.in/amp/story/science-technology/iran-is-threatening-undersea-cables-the-worlds-digital-chokepoints-have-never-been-more-vul