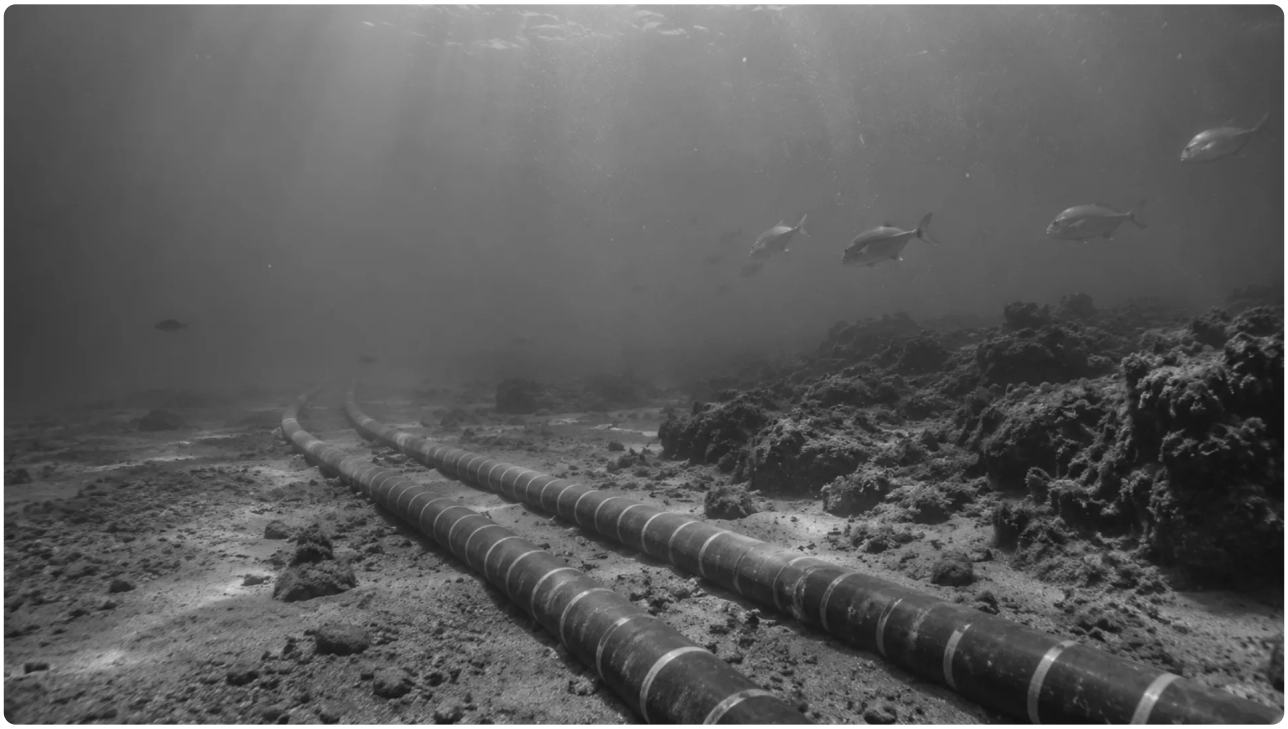
ARTICLES

Undersea Cable Warfare: How Submarine Internet Cables Are Being Weaponized in the Grey Zone

Author: Sharon Ekka • **Published:** July 07, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Submarine cable chokepoints such as the Red Sea–Egypt corridor have become structurally ideal tools for grey?zone information warfare, because they are geographically concentrated, easy to sever with plausible deniability, and protected by an outdated legal framework (especially UNCLOS) that focuses on accidents rather than intentional sabotage, leaving states like India exposed and under?prepared despite growing dependence on these "digital arteries." India must pioneer a dedicated cable-protection doctrine that blends geographical route diversity with active naval monitoring, ensuring that the invisible lifelines sustaining the modern world do not vanish into the shadows of the deep.

Why Submarine Internet Cables Matter to Global Security

Submarine fiber-optic cables are the physical infrastructure of the world's Internet, lying at the depths of the ocean, hidden from our naked eyes. They are not just a technical infrastructure, but they are the very bridges that connect the intercontinental digital exchange. Among these," digital arteries" Red sea-Egypt is one of the most critical nodes connecting data and telecommunication between Asia, Europe, Africa and the Middle East. The dense cluster of cables passing through this narrow artery of the Red Sea makes it a global chokepoint for data, funneling a very large

percentage of Europe - Asia Communication

Now imagine that in periods of conflict, such a chokepoint suffers multiple cable faults almost simultaneously. This Egyptian crossing linking the Mediterranean to the Red Sea is already volatile itself. On paper, these may appear as normal maritime accidents: damage caused by anchor drag, fishing activities, or natural seabed disturbance. The result will be immediate, and consequences will unfold like a domino effect. A significant portion of the world's connectivity and telecommunication gets degraded or rerouted, delaying in Global internet Traffic, disruption in the digital Economy ,trade, and in IT sectors and services. The longer the issue remains, it becomes more than a mere technical inconvenience.

Now, what if these sabotages were intentional under the guise of"accidental".Then it becomes a strategic communication crisis with a delay in cross-border data exchange and logistics, impairing the affected region's ability to get real-time information from the outside world. The objective might not be the full digital blackout but to render the target nation to become information handicapped. Compelling them to depend on fewer alternative routes, vulnerable to throttling and delay, and depriving them of a normal flow of economy and communication. In modern-day warfare, this can be used strategically even though it is not an outright declared war. This is what makes cable disruption relevant to Grey Zone Information Warfare.

This vulnerability exists because of the presence of geographic constraints, forcing the cables to cross through narrow chokepoints that can't be bypassed, while an outdated legal framework focusing on accidents rather than deliberate sabotage makes it easier to claim deniability.

This article examines:

1. How can submarine cables at key chokepoints be weaponized to disrupt global connectivity and information flows?
2. Why does such vulnerability persist despite knowing its risks?
3. What does it mean for specific actors like India.

How Undersea Cables Are Being Weaponized in Grey Zone Warfare

These cables are not uniformly distributed across the globe. The geography and the politics have forced them to squeeze through several narrow, limited nexus points across the globe. Some of the major nexuses include the Red Sea–Egypt corridor, the Strait of Malacca and Singapore hub, the Luzon Strait, the South China Sea–Taiwan region, the English Channel and Atlantic landing clusters, and the Baltic approaches.

When we talk about undersea fiber-optic cables being" weaponized" , it is rarely an overt act but it happens more subtly and highly strategic and often covert, deniable operations.

Accidental Cable Cuts or Deliberate Sabotage?

The most common way is through intentional physical damage cloaked as an everyday maritime incident. Since these incidents are very common occurrences, many of these cable nodes lie beneath critical trade routes of merchant ships and fish trawlers. They drop their anchors and drag them across known cable routes, accidentally snagging them all the time. A foreign actor can direct these ships to purposely" lose control" and cripple the communications while claiming a technical or navigational error. The most evident example of this is the case of Taiwan's Matsu Island(Feb 2023), which was plunged into digital isolation after two of its submarine cables were severed by a Chinese-flagged fishing vessel and a cargo ship dragging its anchors. Although these were deemed as normal accidents, many experts claim that it

was deliberate, “gray-zone” harassment , orchestrated by China .

Another example is the frequent cable cuts in the Baltic Sea(October 2023-December 2024),caused by anchor dragging, involving vessels linked to Russia or China. The cables were cut nine times. Both of these cases follow a pattern: a commercial vessel being used as a proxy weapon. Then they drop their anchors, dragging them for miles, hence damaging the submarine cables. And when caught, the ship's operators claim a mechanical malfunction or a navigating error. This repetitive pattern can’t be a coincidence ,all the time.

Undersea Espionage and Data Tapping

Weaponization also means stealing and intercepting data with the use of specialized submarines and Unmanned Underwater vehicles (UUVs) to tap into the cable’s data without severing it. One historical proof is **Operation Ivy Bells** done by the US in the cold war. They modified a submarine to deep dive into the heavily guarded Sea of Okhotsk, and they wiretapped the Secret Soviet Military cable, intercepting unencrypted Soviet communications via electromagnetic induction for a decade without the Soviets knowing.

How Cable Companies and Supply Chains Become Security Risks

Weaponization can also happen at the corporate and regulatory levels by using the undersea surveys of state-backed companies that lay down these cables to gather intelligence regarding naval chokepoints, submarine hiding spots, and defensive infrastructure. This has sparked a huge risk, and the US government has already taken a few actions, such as intervening to block Google and Meta from connecting the Pacific Light Cable Network (PLCN) to Hong Kong due to national security risks. Similarly, they have pressured the Chinese-owned cable firm HMN Tech, from building a $600 million cable connecting Southeast Asia to Western Europe.

Why Submarine Cables Remain Vulnerable

Why Submarine Cable Repairs Are Slow and Costly

The impacts are immediate, but the recovery is slow. The cost of building is very high, and repairing it is slow, tedious, and logistically complex. It requires logistics such as cable ships, trained crews, specialized equipment, favorable weather and permission to work in busy marine routes or politically sensitive waters. In March 2025, when the PEACE cable was cut ,it was estimated to take several months to fix it ,although they fixed it way earlier. Still, the uncertainty of the required time needed to fix can be weaponized. Adversary nations know that a multi-week lag in resources forces the target nation to bleed its economic resources.

The UNCLOS Blind Spot in Submarine Cable Security

The law regarding this issue is mostly cited from Article 113 of UNCLOS(United Nations Convention on the Laws of the Sea which states that damaging the submarine cable is considered a punishable offense if it was done by the ships carrying the flag of its state or a person under its jurisdiction. Also, only the state with the said flagged ships is obliged to prosecute. That means a coastal state like India can’t arrest the crew in international waters if the ship flies a different country's flag. Also, the damage should be done willfully or by negligence.

Two things to highlight here: firstly, this article fails to account for state-backed proxies or deniable sabotage hiding under the cloak of commercial error. Hence, leaving a legal vacuum that adversaries can exploit. Secondly, it fails to mention what to do if the aggressor is a foreign vessel . Then the international community depends heavily on the specific countries to prosecute their own mariners.

Because of this, the Finnish court had to dismiss *Eagle S(Tanker linked to Russia's "shadow fleet") case* in which the tanker dragged its anchor in the Gulf of Finland and plowed the **Estlink 2** subsea cable. As prosecutors couldn't prove the intent.

It says nothing about state?on?state sabotage, military operations, or wartime seabed warfare. Hence, relying on UNCLOS article 113 is like bringing the 19th C.E. maritime rulebook to the 21st C.E. Hybrid Warfare.

Why Seabed Sabotage Is Difficult to Detect and Prove

Most of the cable faults are genuine accidents like commercial fishing or natural seabed disturbance, which occur throughout the year. Globally, approx. 150 to 200 submarine cable faults happen every year.The deliberate sabotage blends seamlessly in the mix. There is inherent ambiguity at the ocean floor that hides their tracks.

This juncture of structural delays, geographic congestion, and legal weakness ensures that the seabed sabotage retains its essence of low-risk, high-reward type strategy without triggering overt military aggression.

Why Satellites Cannot Replace Submarine Internet Cables

Now the question may arise that if hostile actors cut our undersea cables, then can't the satellites just fill the gap? The answer is no, we can't just switch the global internet over to Starlink,Kuiper, or military satellites. The capacity of this undersea grid to carry the majority of the international communication far exceeds that of satellites. Just one out of 8 fiber pairs alone has a bandwidth of 26.2 (Tbps) than the hundreds of LEO (Low-Earth-Orbiting) satellites combined.

It also has lower latency. Even with modern LEO satellites, a signal must travel from ground terminal to space and then bounce back and forth between satellites, and then finally it travels back down to the ground station on a different continent. From there, it's transmitted to local networks. It might be unnoticeable while doing trivial tasks, but this minor delay can affect high-frequency financial trading systems and defense radar systems. But even depending on satellites for temporary patch can open the risk of swapping state vulnerability to corporate vulnerability. As seen in the Crimea Episode, it showed that a single private company's decision can override a nation's military communication needs.

Hence, the assumption of having satellites to fall back on during an emergency is mistaken. As it may keep essential services alive, but they cannot absorb the immense demand of cloud platforms, streaming, financial exchanges, data center replication, and mass consumer internet traffic across entire continents daily. Therefore, Satellites are like a temporary patch rather than a substitute. The real foundation of our digital world is still undersea cables.

India's Vulnerability to Undersea Cable Disruption

India is one of the largest consumers of mobile data globally, and it is the backbone of the world's IT services. Hence, international cables ought to route their network through India. This gives New Delhi regulatory leverage over how tech companies build their infrastructure in India. In addition to that, the Indian Naval power over the Indian Ocean region effectively supervises the maritime international data traffic between Europe and East Asia. The foreign nations depend on India for the security of these cables.

Despite this leverage, India faces internal and external vulnerabilities. India's westbound data is dependent on the highly volatile Red Sea- Egypt corridor, while its eastbound data traffic is totally dependent on the Malacca Strait and the Singapore Hub. That means even though the internet and telecommunication transmissions are easily accessible to India, if there is a conflict or a deniable 'accident' occurring miles away, it instantly degrades India's domestic internet capacity.

Also, the overwhelming majority of India’s international subsea cables land in Mumbai on the west and in Chennai on the east. This creates a local vulnerability nexus for India. That is, a coordinated cyber-attack, naval blockade, or even a severe localized natural disaster hitting near Mumbai or Chennai landing stations can directly cripple India’s global connectivity, freezing financial trade and national security communications.

Why India Needs a Submarine Cable Protection Doctrine

Currently, the overwhelming majority of India's international subsea cables land at just two primary clusters: **Mumbai (west coast)** and **Chennai (east coast)** ,which means India has two separate routes to backup its data, which are vulnerable to any covert or overt attack, which will directly impact locals. Governments should incentivize companies to build alternative landing sites along the vast coastlines of India(Kochi, Vishakhapatnam, ANI, etc.). It may be expensive, but good for the long term.

India's data traffic is highly dependent on two massive global bottlenecks: the Red Sea/Egypt corridor to reach Europe, and the Strait of Malacca to reach East Asia. But both routes go through similar geographic trenches where they are piled up in clusters. Hence, it is a susceptible risk to India’s digital landscape. India needs to work on projects that will bypass these areas. For Example, emerging Arctic routes could eventually offer a partial bypass.

Cable protection should be treated as a strategic infrastructural policy and not just a telecom policy that unites private telecom operators, internet service providers, and the Ministry of Defense. Ensuring National Security protocols or joint investigations whenever the cable is severed. Also, the framework should take inspiration from the NATO Model launched in 2025 with respect to the repetitive Baltic incidents. It combines naval patrols, satellite surveillance, and automated vessel tracking over undersea corridors. It also frames adversaries, dropping anchor near the cable as a hostile act. India should use existing maritime surveillance networks, specifically the Information Fusion Centre for the Indian Ocean Region (IFC-IOR), to explicitly monitor seabed infrastructure.

On an international level, the UNCLOS articles are long overdue for an update. Nations must establish international protocols that allow evidence sharing and joint forensics. Also, cable sabotage must be integrated as a punishable offence. An intentional deniable attack must trigger a unified security response and collective economic sanctions.

Also, the **EU action plan on Cable Security(Feb,2025)** can be used as a benchmark. This framework bridged the gap between private tech companies and state militaries. It treats subsea cables as critical national security hardware.

The Ocean Floor Is the New Grey Zone Battlefield

Submarine fiber optics cables are an intricate tapestry of a network deeply embedded beneath the surface, buried under endless oceans of the world. Obscured to naked eyes but a vital element for us to survive in this world. It’s the lifeline of the modern digital economy, and their chokepoints have been exploited by the adversaries quietly and deniably. These cable grids are not just important for the vast amount of intercontinental data it transmits, but also because it is now being skillfully weaponized and are being used in hybrid warfare of today’s world. The outdated UNCLOS law and lack of legal framework regarding its protection has transformed the ocean floor into a primary battleground for grey-zone information warfare. Ultimately, it's up to us to protect this silent battleground to safeguard our nation’s economy, military data and communications. For in the age of Hybrid warfare, these arteries can suffocate the today’s world as well as vitalize it.

References:

1. Murphy, Erin, and Thomas Bryja. "The Strategic Future of Subsea Cables: Egypt Case Study." Center for Strategic and International Studies (CSIS). November 2025. https://www.jstor.org/stable/pdf/resrep73012.pdf
2. TeleGeography. *Submarine Cable Map 2025.* 2025. https://submarine-cable-map-2025.telegeography.com
3. Vikramaditya, Captain K.S. "A Collaborative Indo-Pacific Architecture for the Protection of Critical Maritime Infrastructure." *National Maritime Foundation.* June 2, 2026. https://maritimeindia.org/a-collaborative-indo-pacific-architecture-for-the-protection-of-critical-maritime-infrastructure/
4. Burnett, Douglas R. "Submarine Cable Security and International Law." *International Law Studies* 97, no. 1 (2021). Naval War College, Stockton Center for International Law. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3099&context=ils
5. Romaniuk, Scott N., and Amparo Pamela Fabe. "Digital Lifelines: Undersea Cables, Chokepoints, and the Evolving Sea Lines of Communication." *Eurasia Review.* December 26, 2025. https://www.eurasiareview.com/26122025-digital-lifelines-undersea-cables-chokepoints-and-the-evolving-sea-lines-of-communication-analysis/
6. United Nations. *United Nations Convention on the Law of the Sea*, Part VII, Article 113. Opened for signature December 10, 1982. Entered into force November 16, 1994. https://www.un.org/depts/los/convention_agreements/texts/unclos/part7.htm

The views expressed are those of the authors and do not represent the views of CNAWS.

Image Source: ChatGPT