

A Digital Artery in a Minefield.. What Do We Know About Gulf Cables Beneath Hormuz?

Above the surface of the Strait of Hormuz, the picture looks familiar: oil and gas tankers pass daily through one of the most important chokepoints in the energy trade. But underwater lies another invisible layer that forms a vital artery for the digital world.

Beneath this passage run subsea fiber-optic cables, part of a global network carrying about 99% of international internet traffic, including massive financial transactions, cloud data center traffic, and artificial intelligence projects.

These cables connect the Gulf states to the world and power an intertwined economic infrastructure that includes banks, airports, stock exchanges, and government services. As tensions around Iran escalate, the cables have emerged from the shadows to the forefront of risk.

Alongside threats to shipping and energy, talk has begun about the possibility of turning this digital infrastructure into a pressure card through fees, maintenance, or disruption. So what do we know about these cables?

A map of digital arteries on the floor of Hormuz

Subsea cables are fiber-optic lines wrapped in insulating materials and laid on the seabed. In shallow or high-risk sections, they may be buried to protect them from anchors and fishing.

These cables form the backbone of the international internet, providing low latency and enormous capacity, while satellites remain only a backup network with just a small fraction of the available capacity.

In the Strait of Hormuz and its vicinity, there are three active systems that cross Hormuz directly, while other estimates speak of five segments or systems if branches and Gulf-linked cables are included.

Asia Africa Europe-1 (AAE-1): connects Southeast Asia and the Middle East to Europe via the Gulf of Oman and then the Strait of Hormuz, landing in Fujairah, Doha, and Jeddah, and is one of the longest systems (25,000 km).

FALCON: crosses the Red Sea and the Gulf to link India and Egypt through stations in Doha, Dubai, Bahrain, Kuwait, Jeddah, Seeb, and Bandar Abbas.

Gulf Bridge International (GBI): a Gulf-owned regional ring linking Bahrain, Kuwait, Qatar, the UAE, Saudi Arabia, Iraq, Iran, and India.

Branches from longer cables such as SEA-ME-WE 5 and Tata TGN-Gulf.

There are also cables that do not cross the strait directly but still serve the Gulf. Tata TGN-Gulf: one of the regional cables that serves connectivity for the Gulf states.

SEA-ME-WE 5 branch: branches from Oman's Qalhat to Yanbu in Saudi Arabia and Fujairah in the UAE.

The SEA-ME-WE 6 Gulf (Al Khaleej) extension, expected to enter service during 2026, will link Bahrain with Oman, Qatar, and the UAE to provide an alternative internal route.

Other major systems such as 2Africa Pearls, EIG, and Blue-Raman bypass the strait via the Gulf of Oman or the Red Sea, providing extra capacity and options, but they do not eliminate Hormuz's importance.

The cable game.. a digital pie with no single owner

No single country owns subsea cables. Most systems are joint ventures bringing together global telecom companies, governments, and regional operators.

AAE-1, for example, is owned by a group of companies including China Unicom, Ooredoo, center3, Etisalat/e&, Omantel, PCCW, Reliance Jio, and others.

FALCON, meanwhile, is owned by Global Cloud Xchange (FLAG), while GBI is wholly owned by Gulf Bridge International.

Even regional cables such as TGN-Gulf are operated by an Indian company, Tata Communications, with local landing partners in Bahrain, Oman, Qatar, Saudi Arabia, and the UAE.

These cables terminate at landing stations in multiple countries, allowing connectivity sources to be diversified and capacity to be shared. Ownership alliances also mean that decisions on maintenance and upgrades are made collectively, reducing any one country's ability to impose absolute control or use a cable as a political weapon.

Cable maintenance is usually entrusted to specialized companies such as Dubai-based e-Marine, and depends on a limited number of repair ships worldwide.

This distribution of ownership and management makes it legally and technically difficult for any one country to impose fees or unilateral measures on a cable that does not terminate on its territory.

Iran waves the threat of fees on "digital transit"

During the spring of 2026, proposals were published by the Iranian agencies Tasnim and Fars calling for three measures on cables crossing the Strait of Hormuz, most notably:

Collecting licensing or renewal fees from foreign companies.

Obliging major technology companies such as Google, Meta, and Microsoft to comply with Iranian laws.

Granting Iranian companies exclusive rights to maintain the cables.

These arguments were based on the idea that Iran has sovereignty over the “hidden route” beneath the strait and could use the cables as leverage. But the proposals remained media talking points and did not take shape as official policy.

Experts in law and telecommunications confirmed to The Guardian that the buried cables pass through international waters or Omani territorial waters and do not terminate on Iranian soil.

That makes the imposition of broad Iranian fees on the cables legally complex, because the freedom to lay cables is guaranteed under international law, while the coastal state’s powers remain constrained by the principles of necessity and proportionality.

Even delaying maintenance could backfire on Iran, since its own digital infrastructure also depends on these cables. That is why the Iranian threat appears more like a political card than a practically enforceable measure.

The nightmare of disruption.. the 40-day journey

Despite fears of sabotage, data indicate that around 70–80% of global faults are caused by anchors, fishing, and trawling, while deliberate incidents account for no more than 1%. Between 150 and 200 incidents occur each year, and earthquakes and landslides cause about 10% of outages.

Repairing a cable is a complex process involving several stages illustrated in the following infographic.

This process usually takes 40 days or more because of administrative procedures to obtain permits to enter territorial waters and the technical preparations involved, and it costs between \$1 million and \$3 million per incident.

The global repair fleet does not exceed 60–80 vessels, of which only 2–4 are in the Middle East, creating time bottlenecks, especially if several faults occur simultaneously.

In conflict zones, repairs may be delayed for months because of security risks and difficulty obtaining permits, as happened in the Red Sea in 2024.

As for the Strait of Hormuz, the seabed’s rocky terrain and strong currents make burying cables difficult, so operators prefer to bury them in the more suitable Omani waters.

The greatest danger lies not in cutting the cable itself, but in disrupting repair operations or obstructing ships from reaching the fault zone.

The Gulf.. \$10 trillion at risk

Most Gulf states are building digital economies that depend on high-capacity international connectivity and low latency.

The UAE has more than 35 data centers and hosts global cloud companies.

Saudi Arabia has around 20 data centers and is investing in an AI complex with 6 gigawatts of capacity.

Qatar has 5 data centers and is planning major AI projects.

These centers are linked through Hormuz to global markets and secure the operations of banks, airports, and government agencies.

Qatar, Bahrain, and Kuwait are among the countries most exposed to any cut in Hormuz because they rely on a limited number of subsea cables and do not have major overland routes.

That is why cable disruption could slow banking transactions, increase latency, disrupt airport, cloud, and data center services, and force companies to reroute traffic through alternative paths with lower capacity or higher cost.

Even countries with multiple alternatives, such as the UAE and Saudi Arabia, face risks of higher latency and lost capacity if Hormuz cables are disrupted at the same time as faults in the Red Sea.

Global banking networks are estimated to process about \$10 trillion a day through these cables, showing that slowdown or disruption would affect trade and financial markets, not just consumer internet.

Overland and maritime alternatives fraught with explosives

The Gulf states share several alternative routes to reduce reliance on the Strait of Hormuz, but each has its limits.

Gulf of Oman and the Red Sea: many cables head first into Omani waters and then cross the Red Sea. Systems such as EIG, 2Africa, and Sea-Me-We 6 therefore provide alternative connectivity via the Red Sea and Egypt. But tensions in Yemen and attacks on ships led to several cable cuts in 2024 and delayed their repair, so any simultaneous fault in the Red Sea and Hormuz could create a double bottleneck.

Overland routes: there is the MEETS network, stretching 1,400 km along GCC power lines and providing initial capacity of 200 Gbps, and the SNFN network, which links Saudi cities and extends to Jordan, the UAE, Qatar, Bahrain, Kuwait,

Iraq, and Oman. But these routes require supporting infrastructure and sovereign approvals, and may shift risks from sea to land.

New projects: the Saudi-Syrian SilkLink project, spanning 4,500 km, aims to connect the Gulf to Europe via Syria and Turkey, but depends on stability in Syria.

The WorldLink project seeks to lay a cable between the UAE and Iraq and then continue overland to Turkey at a cost of \$700 million, but it has not yet begun.

Fibre in the Gulf (FIG) plans to build a cable with a capacity of 720 Tbps to connect the Gulf states, while the Al Khaleej cable extension will add an internal route within the Gulf, and 2Africa Pearls will bring massive capacity and reach every Gulf state by 2026.

These latest projects promise to reduce risks, but they are not yet ready or face political and security challenges, and on their own they are not enough to absorb the full current capacity.

That is why the Gulf states are moving to diversify maritime and overland routes. But these alternatives do not eliminate the fragility of narrow corridors so much as they distribute the risks.