OPTARUS
RISK & INTELLIGENCE

MARITIME INSIGHT

Iran and the Subsea Cable Threat

Capability, opportunity and resilience across the Gulf–Red Sea digital corridor

26 October 2026 | Source review: 26 October 2026

Open-source maritime assessment

ILLUSTRATIVE

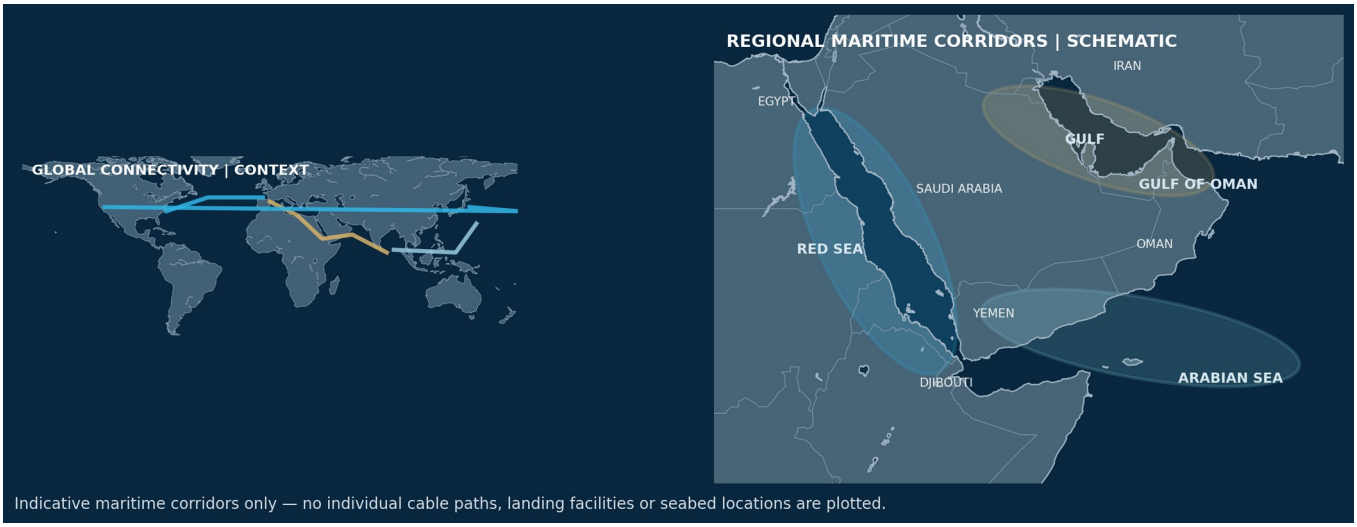


FIGURE 1. Global context and the Gulf–Red Sea regional operating picture. Optarus original generalised map; NOT precise cable alignments or landing-point data. Corridor geography informed by TeleGeography [4].

Iranian officials have publicly threatened Gulf undersea communications infrastructure, while two unnamed security officials described contingency planning to Reuters. That establishes a credible coercive signal, not verified specialised sabotage capability. The ICPC identifies five active cable-system segments traversing Hormuz; Iranian statements referring to seven should not be treated as a validated inventory. With less than 1% of international bandwidth traversing Hormuz, the likely consequences of a successful attack are concentrated on Gulf connectivity and dependent international services, not a global internet shutdown. Rerouting may preserve access but raise latency, congestion and cost; sustained interruption becomes more plausible if multiple routes fail or conflict prevents repairs. [1–3,6,13,14]

>99%	<1%	23.4 DAYS	7.7 DAYS
Intercontinental data traffic via subsea cables [5]	International bandwidth via Hormuz [3]	2025 mean notification-to-departure [6]	2025 mean vessel transit [6]

Evidence status: on-record threat CONFIRMED | operational plans REPORTED, UNVERIFIED | capability UNPROVEN | effects SCENARIO-BASED

CURRENT THREAT PROFILE

What changed, and how strong is the evidence?

DATE / SOURCE	REPORTED DEVELOPMENT	EVIDENCE STATUS
19–21 Oct | Iranian state / regional media [1,2]	Iranian officials threatened seabed data infrastructure; rhetoric cited seven cables, whereas ICPC identifies five active Hormuz segments. [1,2,14]	On-record threat; seven-cable claim is inconsistent with ICPC's five active segments. No action verified.
23 Oct | Reuters [3]	Two unnamed Iranian security officials said plans existed for cable attacks; one suggested obstructing repairs.	Credible reporting of claims, but officials were unnamed and no corroborating operational evidence supplied.
Sep–Oct | MARAD / UKMTO [9,10]	Official maritime notices document threats and attacks against merchant vessels in Gulf waters.	Demonstrates a contested maritime environment; does not prove subsea cable attack capability.

Means • opportunity • motive: separate the three tests

TEST	SUPPORTED ASSESSMENT	LIMIT / COUNTER-INDICATOR
MEANS	Iran has maritime strike and coercive capacity against shipping [9]; this is relevant to the security environment around cable operations.	It does not establish specialised ability to reach, identify, disrupt or repeatedly damage buried or deep-water communications infrastructure.
OPPORTUNITY	Proximity to Gulf waters offers geographical access; conflict could constrain survey/repair access and commercial vessel activity.	Surveillance, maritime patrols, territorial permissions and repair-provider precautions complicate access. Naval presence is not evidence of a cable-specific mission.
MOTIVE	A conditional threat could increase pressure on Gulf governments, investors, cloud operators and Washington by widening the perceived cost of renewed conflict.	Escalation would also risk reputational, diplomatic and economic costs to Iran and regional customers; signalling need not imply execution.

What cable damage would physically mean

Subsea fibre-optic cables are physical seabed infrastructure. Physical disruption could involve interference associated with vessels or anchors, direct tampering with the cable system or interference with connected shore infrastructure; deliberate seabed operations would require additional specialist knowledge and access. Damage to a cable does not necessarily cause an end-to-end service outage because network operators can move traffic to alternative routes. Different water depths, burial, armouring, seabed conditions, surveillance and repair access affect feasibility; no single attack method or success rate can be inferred for the Gulf. Industry evidence shows accidental anchor and fishing incidents dominate global cable faults, not proven hostile activity. Iranian claims of easy access do not establish an operational capability. [3,13,14]

ANALYTICAL BOUNDARY

No open-source material reviewed demonstrates an Iranian test against a specific Gulf cable or confirms a deployed system designed for multi-cable seabed attacks. This assessment deliberately excludes coordinates, precise cable alignments, landing sites, seabed-depth targeting data and procedural sabotage methods. These details are not necessary to judge commercial exposure.

Maritime protection and escalation

US and partner warships contribute to wider maritime security, force protection and deterrence. No reviewed official notice demonstrates that their primary task is defending seabed cables. Patrols can complicate hostile access, but cannot continuously secure every cable segment. Coordinated surveillance, rapid operator fault verification, safe repair-vessel access and authorisations are more relevant to restoration resilience. [9,10,12,14]

MARITIME OPERATING PICTURE

A physical cut is not equivalent to loss of the internet

Internet paths are diverse. Operators may reroute onto other subsea systems, terrestrial cross-border links and cached/local content. Whether users notice an outage depends on the spare capacity and independence of those paths, local interconnection and cloud-service dependencies. Rerouting can preserve reachability while increasing delay, congestion and packet loss. It cannot create unlimited replacement capacity. [7,8]

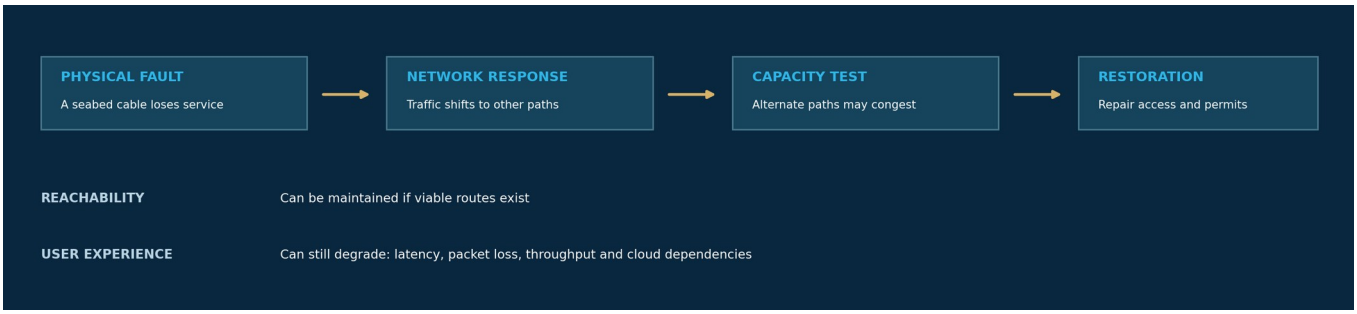


FIGURE 2. Distinguishing physical cable restoration from logical service continuity. Optarus schematic based on the ITU, ICPC and Internet Society [5–8].

Historical tests of resilience: evidence, not forecasts

CASE	OBSERVED OUTCOME	WHAT IT DOES / DOES NOT SHOW
East Africa, May 2024 [7]	Two cables failed; no total national internet shutdown across affected countries. Alternatives congested; both cables were restored by 3 June, around three weeks later.	Proves adaptation is possible, but restoration timing cannot be transferred to a conflict-affected Gulf.
Red Sea, Sep 2025 [8]	Multiple fibre faults produced higher Middle East transit latency; Microsoft rerouted Azure traffic without a complete network interruption.	Demonstrates service continuation with performance penalty, not immunity of every provider or customer.
ICPC global 2025 [6]	178 repairs; mean 23.4 days from notice to vessel departure and 7.7 days from sailing to worksite.	These are averages BEFORE repair; not a promise of restoration within 31 days.

Recovery windows: scenario assessment, not predictive deadlines

SCENARIO	SERVICE EFFECT / TIMEFRAME	RESTORATION LIMIT
One system damaged; diverse spare routes available	Some services could reroute in minutes/hours; capacity rebalancing may take longer.	Seabed repair may still take weeks; users can recover before the cable does.
Several regionally correlated failures	Congestion, impaired cloud access and increased latency can persist for days or weeks, depending on available alternatives.	Repair priorities, number of vessels and regional permissions become binding.
Faults plus contested repair access	Localized disruption/degradation could persist many weeks or longer under adverse conditions.	No defensible fixed upper bound; escalation could block vessels, insurers or permits.

Timing estimates are illustrative analytical ranges, not quantified forecasts. They should not be added together or interpreted as guaranteed service restoration intervals.

GEOGRAPHICAL EXPOSURE | Europe and the wider world

The location of damage matters more than the nationality of the party responsible. A Hormuz-specific incident primarily affects Gulf-connected networks; a separate, larger Red Sea transit disruption would have greater potential to degrade Europe–Asia paths. These are distinct scenarios, not one assumed Iranian capability. European domestic connectivity, online banking and cloud services should not be described as generally at risk of failure. The exposure is narrower: particular international transactions, cross-region cloud transfers, real-time applications and providers with insufficient independent paths. [3,7,14–16]

EXPOSURE	ASSESSMENT UNDER A HORMUZ-FOCUSED CABLE-DAMAGE SCENARIO
Gulf states	Highest direct exposure: local ISP transit, cross-border cloud or payment dependencies, port and logistics platforms. Effects vary materially by redundancy.
Wider MENA / South Asia	Selective congestion or slower international routes possible where carriers rely on affected interconnections; not a uniform regional outage.
UK / Europe	Most likely indirect or route-specific latency, packet loss and application degradation on Gulf/Asia-linked traffic; domestic access generally expected to continue.
Elsewhere	System-wide interruption not supported; individual global businesses may still have concentrated dependencies on regional hosts or networks.

OBSERVED EUROPE–ASIA LATENCY | September 2025 Red Sea cuts

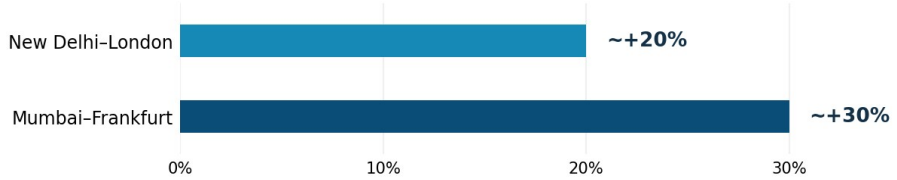


FIGURE 3. Cloudflare probe-measured change in mean latency after the September 2025 Red Sea faults; two specific India–Europe links only. Historical observation, NOT a forecast for a Hormuz incident. [15]

Cisco ThousandEyes separately observed that service on an AWS Mumbai–Frankfurt route returned near baseline after roughly eight days of traffic optimisation, before necessarily completing physical repairs. This is evidence of adaptive reconfiguration, not guaranteed spare capacity or recovery time. [16]

COMMERCIAL EXPOSURE

Transmission disruption becomes a business-continuity problem

Gulf financial services and payments, trading systems, logistics platforms, ports, aviation, health services, government networks and data-centre operators may experience uneven effects. Some remain available through redundant routes; others reliant on constrained international transit, particular cloud regions or remote authentication could degrade. Secondary impacts include higher transit procurement costs, backup-capacity demand, service-level disputes, repair-vessel insurance and prolonged operational uncertainty. The impact is determined by each operator's dependency architecture, not by an assumed region-wide blackout. [3,5,7,8,11,12]

MONITORING VALUE | KASPR Pulse

KASPR Pulse measures district-level responding IPv4 connectivity, round-trip latency and jitter and supplies historical baselines and anomaly flags. It offers a potential independent indicator of geographically uneven service degradation, provided readings are compared within the same area over time. The public Regional Intelligence page does not establish a current Iranian cable incident or demonstrate a causal link to any submarine system. ICMP sampling excludes unresponsive addresses and cannot, on its own, attribute a cable fault; operator notices, network-route measurements and repair advisories remain essential corroboration. [17]

Competing outcomes and confidence

ANALYTICAL OUTCOME	ASSESSMENT / CONFIDENCE
Coercive signalling without seabed attack	Consistent with conditional public rhetoric; future actions cannot be inferred from statements alone. MODERATE.
Limited physical fault with rapid logical rerouting	Plausible where geographically distinct spare paths and peering exist. MODERATE.
Multi-fault event compounded by repair denial	Higher consequence but depends on unverified capability, intent and opportunity. LOW.
Generalised global internet shutdown	Not supported by Hormuz bandwidth data or network topology. HIGH confidence in rejection.

Priority indicators and decision thresholds

Escalation indicators: independently verified cable-fault advisories or operator notices; simultaneous route-performance anomalies across unrelated carriers; corroborated deployment or interference affecting repair vessels; changes to repair permissions or war-risk coverage; sustained shortfalls in spare capacity. De-escalation indicators: evidence of intact systems, normalised service metrics, granted repair access, independent alternate paths and formal withdrawal of threats. Attribution should remain open unless physical evidence, operator data and independent official assessments converge.

BOTTOM LINE

Treat the Iran cable threat as a credible coercive signal with uncertain specialised capability. The decision-relevant exposure is not a guaranteed worldwide outage: it is the resilience of each organisation's actual networks, the availability of genuinely independent paths, and the security and regulatory conditions under which any physical fault could be repaired.

SOURCE APPENDIX | Selected originating and specialist sources

[1] Press TV / Al-Alam, Javani interview, 21 Oct 2026 — presstv.co.uk/Detail/2026/10/21/778862/
[2] IranWire, IRGC spokesman's warning, 20 Oct 2026 — iranwire.com/en/news/159089-irgc-threatens-undersea-internet-cables-in-strait-of-hormuz/
[3] Reuters, interviews with two Iranian security officials, 23 Oct 2026 — reuters.com/world/middle-east/iran-has-detailed-plans-hit-gulf-undersea-cables-if-war-resumes-officials-say-2026-10-23/
[4] TeleGeography, 2026 Global Submarine Cable Map — resources.telegeography.com/2026-submarine-cable-map (694 in-service / planned systems).
[5] ITU / International Advisory Body, global cable-resilience recommendations, 10 Jul 2026 — itu.int/en/mediacentre/Pages/PR-2026-07-10-Submarine-cable-resilience-report.aspx
[6] ICPC, 2026 Plenary Highlights: 2025 repair dataset — iscpc.org/events/2026-plenary-meeting/
[7] Internet Society, 2024 East Africa cable-outage report, 23 Jul 2024 — internetsociety.org/resources/doc/2024/2024-east-africa-submarine-cable-outage-report/
[8] Microsoft Azure, 6 Sep 2025 incident update (archived) — isdown.app/status/azure/incidents/441417-multiple-subsea-fiber-cuts-in-the-red-sea-impacting-global-communications
[9] US MARAD, Advisory 2026-011, 9 Sep 2026 — maritime.dot.gov/msci/2026-011-persian-gulf-strait-hormuz-and-gulf-oman-iranian-attacks-commercial-vessels
[10] UKMTO, Oct 2026 recent incident warnings — ukmto.org/recent-incidents
[11] Ooredoo Oman, Salalah data centre/cable landing infrastructure, 17 Aug 2025 — ooredoo.om/en/press-release/ooredoo-launches-salalah-data-centre-to-strengthen-omans-role-as-a-regional-digital-hub/
[12] European Commission, Submarine Cable Security Toolbox, 5 Feb 2026 — digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest
[13] ICPC, Media enquiries and FAQs: fault risk and water depth — iscpc.org/news/media-enquiries/
[14] ICPC, Strait of Hormuz media FAQs (five active cable segments; resiliency), 20 May 2026 — iscpc.org/news/media-enquiries/
[15] Cloudflare Radar, Q3 2025 Internet Disruption Summary: Red Sea cuts, India–Europe probe latency — blog.cloudflare.com/q3-2025-internet-disruption-summary/
[16] Cisco ThousandEyes, The Internet Report, Sep 2025: route performance and post-cut optimisation — thousandeyes.com/blog/internet-report-starlink-google-maps-sdk-outages
[17] KASPR Pulse, Regional Intelligence and data documentation (accessed 26 Oct 2026) — pulse.kasprdata.com/applications/regional; pulse.kasprdata.com/data/documentation

METHODOLOGY / LIMITATIONS: Open-source assessment using material reviewed on 26 October 2026. Evidence distinguishes on-record threats, anonymous claims, operational capability and scenario effects. Figures 1–2 are generalised schematics and do not represent exact cable routes or attack locations. Figure 3 is historical and route-specific. No attack, sabotage attribution or present cable fault is asserted. KASPR is discussed as a measurement framework, not treated as verified incident data. AI assisted research and presentation; source evaluation and publication decisions remain Optarus editorial responsibilities.