AL HABTOOR RESEARCH CENTRE

Securing the Arabian Gulf's Subsea Cables:

The Iranian Threat, Defence Options, and Digital Resilience

OCTOBER 2026

AL HABTOOR RESEARCH CENTRE

Securing the Arabian Gulf's Subsea Cables:

The Iranian Threat, Defence Options, and Digital Resilience

OCTOBER 2026

Dr. Azza Hashim

Managing Director of Al Habtoor Research Centre

BY

Mostafa Ahmed

Head of Political and Security Studies Unit

Al Habtoor Research Centre seeks to be a leading centre of excellence in political and economic studies and early warning in the region. Our vision is to advance informed, evidence-based policy and decision-making that drives sustainable development, strengthens institutions, and reinforces regional peace and stability. We are committed to delivering innovative solutions to the region's most pressing challenges through research, analysis, and dialogue.

CONTACT US

info@habtoorresearch.com · www.habtoorresearch.com

Contents

Introduction....1

Threats and vulnerabilities in Hormuz....2

A layered framework for cable protection....6

Connectivity alternatives....9

Crisis management and response scenarios....13

A forward programme for crisis readiness....15

Conclusion....17

References....18

Figures and tables

Table 1. Submarine cable systems....3

Figure 1. Cable corridor and communications facilities....4

Figure 2. Sensing, surveillance and protection....6

Figure 3. Maritime gateways and terrestrial links....10

Table 2. Comparing connectivity options....12

Introduction

Iranian threats in October 2026 to target submarine fibre-optic cables and cloud computing centres in the Arabian Gulf and the Strait of Hormuz added a further security dimension to the calculations surrounding any potential military escalation in the region. As Gulf Cooperation Council (GCC) economies expand their digital financial services, hyperscale cloud computing and sovereign artificial intelligence capabilities, telecommunications infrastructure has become more than a means of transmitting data. It now underpins the continuity of businesses, markets, supply chains and operational systems in the energy sector.

Assessing this threat requires a distinction between political rhetoric and technical and operational realities. The shallow waters of the Arabian Gulf and the narrow shipping lanes of Hormuz create physical vulnerabilities that expose cables and landing stations to grey-zone operations or direct attack. Yet damage to a submarine cable or a cloud facility does not necessarily produce comprehensive paralysis or a complete loss of connectivity. The shared character of intercontinental cable networks also imposes constraints on Tehran itself: Iranian connectivity and the interests of its Asian partners depend on the same maritime routes. Gulf networks can, moreover, contain the impact when alternatives have been tested in advance.

This paper provides a technical and strategic assessment of the scale and geographical limits of the threat, examining potential methods of attack on the seabed and on land. It moves from identifying vulnerabilities to outlining a practical framework for layered defence and deterrence that combines fibre-optic sensing, physical protection, regional maritime coordination, and legal and diplomatic instruments. It also examines the practical viability and capacity constraints of available alternatives, from maritime bypass routes through the Gulf of Oman and the Arabian Sea and terrestrial links across the Arabian Peninsula to satellite networks, digital islanding and sovereign cloud services. Three scenarios of escalating disruption then assess crisis management and service restoration.

Threats and vulnerabilities in the Hormuz digital corridor

The maritime corridor extending from the Gulf of Oman through the Strait of Hormuz into the Arabian Gulf contains one of the world's densest concentrations of critical energy and digital infrastructure. Seventeen submarine cable systems extend across the Gulf and its approaches. Mapping data from TeleGeography and Submarine Networks identify seven principal cable systems, alongside regional branches and composite links serving local oilfields. Together, these form the principal targets referred to by the Islamic Revolutionary Guard Corps (IRGC) spokesperson in October 2026.

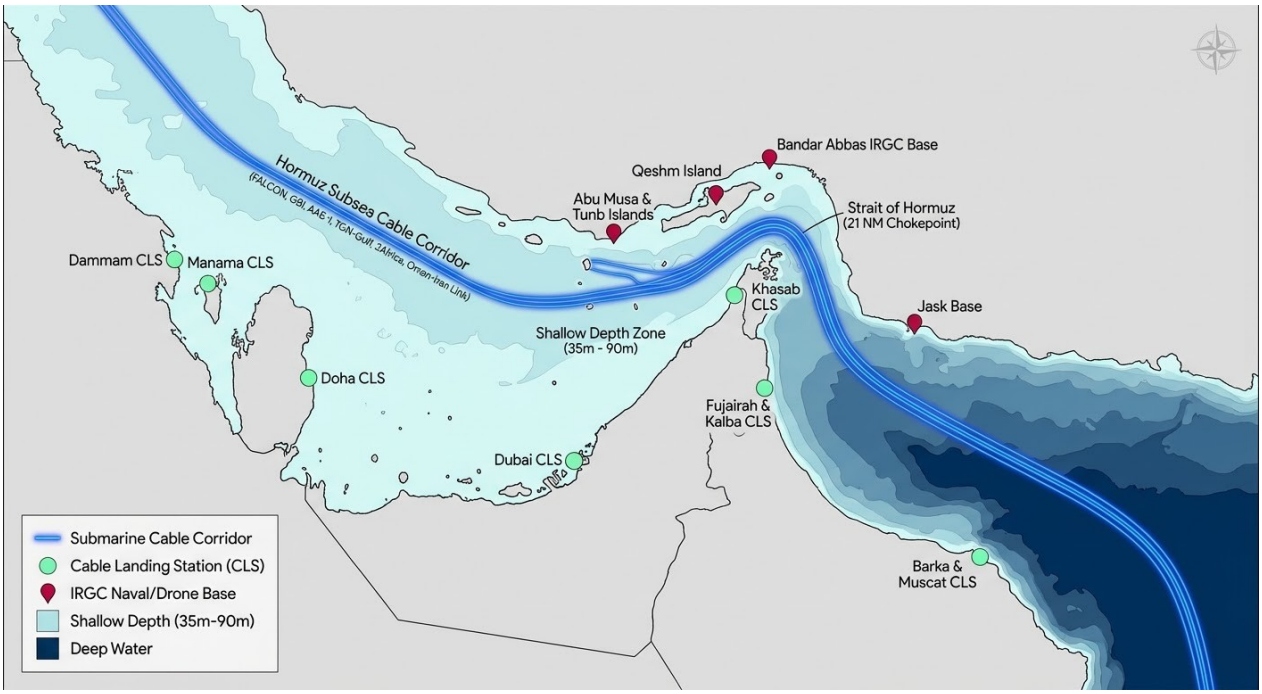
An inventory must distinguish between systems serving the region, operational segments crossing the strait and projects that have yet to enter service. In its statement updated on 20 May 2026, the International Cable Protection Committee (ICPC) identifies five operational segments crossing Hormuz and states that the international bandwidth passing through it accounts for less than 1% of the global total. This does not imply a limited impact on the countries connected to those segments; it distinguishes regional exposure from the strait's share of global connectivity. Table 1 presents systems and links serving the Gulf and its surroundings. Its rows do not represent a count of operational cables within Hormuz, and design capacity is not equivalent to spare capacity available during a crisis.

Table 1. Submarine cable systems, landing points and geographical exposure

Cable system	In service / status	Design capacity and limitations	Main landings inside the Gulf / strait	Main landings outside Hormuz	Owners, consortia and strategic role	Geographical exposure
FALCON (FLAG–Alcatel-Lucent Optical Network)	2006; upgraded	Capacity varies by segment and upgrade. Nominal capacity is not automatically available as reserve.	Dubai (UAE); Doha (Qatar); Manama (Bahrain); Al Khobar (Saudi Arabia); Kuwait City; Bandar Abbas and Chabahar (Iran); Khasab (Oman).	Seeb / Muscat (Oman); Mumbai (India); Suez (Egypt).	Global Cloud Xchange (GCX) and regional operators. A core Gulf ring linking all GCC states and Iran to India and the Red Sea.	High: crosses Hormuz directly and has Iranian landings.
AAE-1 (Asia–Africa–Europe 1)	2017	High international capacity. Available alternatives depend on the branch, contracts and equipment.	Doha (Qatar), via a branch crossing Hormuz.	Fujairah (UAE); Barka (Oman); Aden; Jeddah; Marseille; Hong Kong.	Consortium including Ooredoo, e&, Telecom Egypt, PCCW and China Unicom. A major low-latency Europe–Asia link with a dedicated Gulf branch to Qatar.	High: the main route bypasses Hormuz via Fujairah and Barka, but the Qatar branch crosses the strait.
Gulf Bridge International (GBI)	2012	High-capacity regional ring. Reserve capacity must be measured for each segment.	Doha (Qatar); Al Khafji (Saudi Arabia); Kuwait; Al Hidd (Bahrain); Dubai (UAE); Bushehr (Iran); Al Faw (Iraq).	Fujairah (UAE); Barka (Oman); Mumbai (India).	Operated by carrier-neutral GBI. A high-capacity mesh linking Gulf states internally, with external connectivity through Fujairah and Barka.	High: enters the Gulf through two routes across Hormuz.
TGN-Gulf (Tata Global Network–Gulf)	2012	Enterprise and carrier capacity. Access depends on contractual rights.	Doha (Qatar); Manama (Bahrain); Dammam / Al Khobar (Saudi Arabia); Dubai (UAE).	Fujairah (UAE); Muscat / Barka (Oman); Mumbai (India).	Tata Communications with regional partners e&, Bahrain Internet Exchange, Ooredoo and Mobily. A vital link to India for corporate banking and cloud services.	High: enters the inner Gulf through a single chokepoint.
SEA-ME-WE 5 (South East Asia–Middle East –Western Europe 5)	2016	High international capacity. Terrestrial backhaul capacity to Gulf users requires verification.	Connects to UAE and Gulf backhaul networks through Fujairah / Kalba.	Fujairah / Kalba (UAE); Barka / Muscat (Oman); Djibouti; Yanbu; Toulon; Singapore.	Consortium of 19 global operators, including e&, stc, Ooredoo, Telecom Italia Sparkle and China Mobile. A major intercontinental backbone.	Medium to high: terminates outside the narrowest corridor at Fujairah and Barka, but its approaches remain exposed.
2Africa, including the 2Africa Pearls extension into the Gulf	Status varies by segment. Verify the Gulf extension is operational before counting its capacity.	High-capacity expansion project. Inactive segments must not be counted as emergency capacity.	Kalba (UAE); Doha (Qatar); Manama (Bahrain); Dammam (Saudi Arabia); Kuwait; Al Faw (Iraq).	Barka and Salalah (Oman); Kalba (UAE); Jeddah; Yanbu; Europe / Africa.	International consortium of telecommunications and technology companies. Expands regional connectivity as segments are completed and activated.	Depends on each branch's route and operating status. The whole project should not be treated as an operational cable inside Hormuz.
Oman–Iran links, including POI and FALCON branches	2011–2015	Separate regional links. Capacities should not be aggregated without checking their independence.	Bandar Abbas, Jask and Chabahar (Iran); Khasab (Oman).	Muscat / Barka (Oman); Fujairah (UAE).	Omantel, Iran's Telecommunication Infrastructure Company (TIC) and Pishgaman. Carry a significant share of Iran's international IP transit traffic.	High for segments crossing the strait. These are multiple links, not one system.
Fibre Optic Gulf (FOG) and local coastal links to oil facilities and islands	1998; upgraded	Regional and domestic connectivity. Capacity is not equivalent to an independent international gateway.	Dubai / Fujairah (UAE); Doha (Qatar); Manama (Bahrain); Kuwait City; offshore oil platforms.	Fujairah (UAE).	Consortium including e&, Ooredoo, Batelco/Beyon and Kuwait's Ministry of Communications, supplemented by E-marine composite cables serving offshore oil platforms.	High: exposed in shallow continental-shelf waters along the southern Gulf.

These submarine systems support far more than web browsing, video calls and social media platforms such as Instagram and WhatsApp. They provide the physical infrastructure required to transmit SWIFT interbank financial messages, stock market transactions, sovereign wealth funds' algorithmic trading and the real-time synchronisation of distributed databases across Amazon Web Services (AWS), Microsoft Azure, Google Cloud and Meta platforms. They also support virtual machine migration, internal application programming interface (API) traffic and industrial supervisory control and data acquisition (SCADA) systems linking offshore oil and gas platforms to onshore control centres. Intercontinental trunk systems, including AAE-1 and SEA-ME-WE 5, carry core traffic between Asia and Europe through landing stations on the Gulf of Oman coast at Fujairah, Kalba and Barka. States inside the Arabian Gulf, particularly Qatar, Bahrain, Kuwait, Iraq and Iran, together with Saudi Arabia's eastern coast, depend heavily on regional branches and loops, including FALCON, GBI, TGN-Gulf and FOG, as well as the 2Africa Pearls extension once fully operational. Their exposure to Hormuz varies according to the route and operational status of each segment. As the endpoint of an AAE-1 branch within the Gulf, Qatar faces a particular risk of losing access to international capacity if Hormuz connections are severed and terrestrial networks reach saturation.

Figure 1. Cable corridor and communications facilities around the Strait of Hormuz



The geographical and hydrographic characteristics of Hormuz and the Arabian Gulf heighten this strategic vulnerability, leaving submarine cables particularly exposed to both accidental damage and deliberate sabotage. Unlike transoceanic cables in the Atlantic and Pacific, which lie at depths of 3,000–6,000 metres and can be reached only by a limited number of specialised deep-diving platforms, the Arabian Gulf is a shallow sea over the continental shelf. Its average depth is only 35–50 metres, and depths rarely exceed 90 metres even in the deeper channels along the Iranian coast and through Hormuz. At its narrowest point, between the Musandam Peninsula and Iran, the strait is only 21 nautical miles wide. Commercial shipping is concentrated within two-nautical-mile-wide lanes governed by traffic separation schemes.

This confined maritime geography creates a close physical overlap between commercial shipping at the surface and digital infrastructure on the seabed. Large crude oil tankers and liquefied natural gas carriers pass daily above the same routes occupied by the Gulf's fibre-optic cables. These cables are often no thicker than an ordinary garden hose, typically measuring 17–50

millimetres in diameter depending on their armouring.

During geopolitical crises, naval blockades or electronic warfare involving manipulation of Global Positioning System (GPS) and Automatic Identification System (AIS) signals, dozens of commercial vessels may congregate and anchor in crowded waiting areas, increasing the risk of cable damage from dragging anchors. Tactical geography compounds this seabed vulnerability. Fortified IRGC naval facilities are located along the northern approaches at Bandar Abbas, Jask and Bushehr, alongside forward operating bases on Qeshm, Larak and Hormuz and the three occupied Emirati islands. Cable routes lie only 5–15 nautical miles from some of these island positions, a distance that fast attack craft or small submarines can cover in less than thirty minutes.

Across the spectrum of escalation, the IRGC and Iran's regular navy possess a range of capabilities for hybrid seabed warfare and attacks on infrastructure ashore. One operational approach involves uncrewed underwater vehicles (UUVs), autonomous underwater systems and dormant seabed munitions. Over the past decade, the IRGC Navy has prioritised asymmetric uncrewed maritime systems to offset the conventional naval superiority of the United States and the GCC states. Equipment used in such operations may include side-scan sonar, optical cameras, shaped explosive charges that concentrate blast energy, or hydraulic cable cutters. These systems, together with wire- and fibre-guided coastal munitions developed to defend Hormuz's maritime approaches, can be deployed covertly from traditional coastal vessels, commercial support ships or island bases. They may then lie in wait along mapped cable routes and be activated by a direct command or pre-programmed acoustic signals.

A second, related underwater method centres on Ghadir-class midget submarines, IRGC combat divers and seabed charges. Some shallow segments are accessible to specialist divers, depending on depth, currents and operating conditions. Combat divers from the IRGC Navy's Takavaran special forces may therefore be able to reach unburied or shallow-buried cable sections directly. Platforms potentially used for such operations include Ghadir-class midget submarines and Fateh-class coastal submarines, designed for shallow, acoustically congested coastal waters, to deploy limpet mines, bottom influence mines or swimmer delivery vehicles directly at seabed infrastructure.

A third potential method, for which responsibility can be difficult to establish, is anchor dragging by commercial vessels associated with the "shadow fleet", while retaining plausible deniability. Incidents between 2024 and 2026 demonstrate how submarine cables have become a major arena of hybrid confrontation: uncertainty over whether a fault resulted from an accident, crew negligence or deliberate sabotage complicates deterrence through retaliation. In February 2024, three to four Red Sea cables were severed after a Houthi missile disabled the cargo vessel Rubymar and its anchor dragged across the seabed, disrupting 25% of data traffic between Asia and Europe. In November 2024, two Baltic Sea cables linking Finland to Germany and Sweden to Lithuania were cut. Serious damage to a Sweden–Latvia cable followed in January 2025, and unattributed cuts to two cables near Jeddah in September 2025 impaired internet access across the Middle East and South Asia. Tehran could use an ageing tanker from its sanctions-evading shadow fleet, operating without a flag or under a false flag, to drag a multi-tonne anchor across a group of Hormuz cables under the pretext of engine failure. Several links could be damaged while evidence of intent and responsibility would still be required.

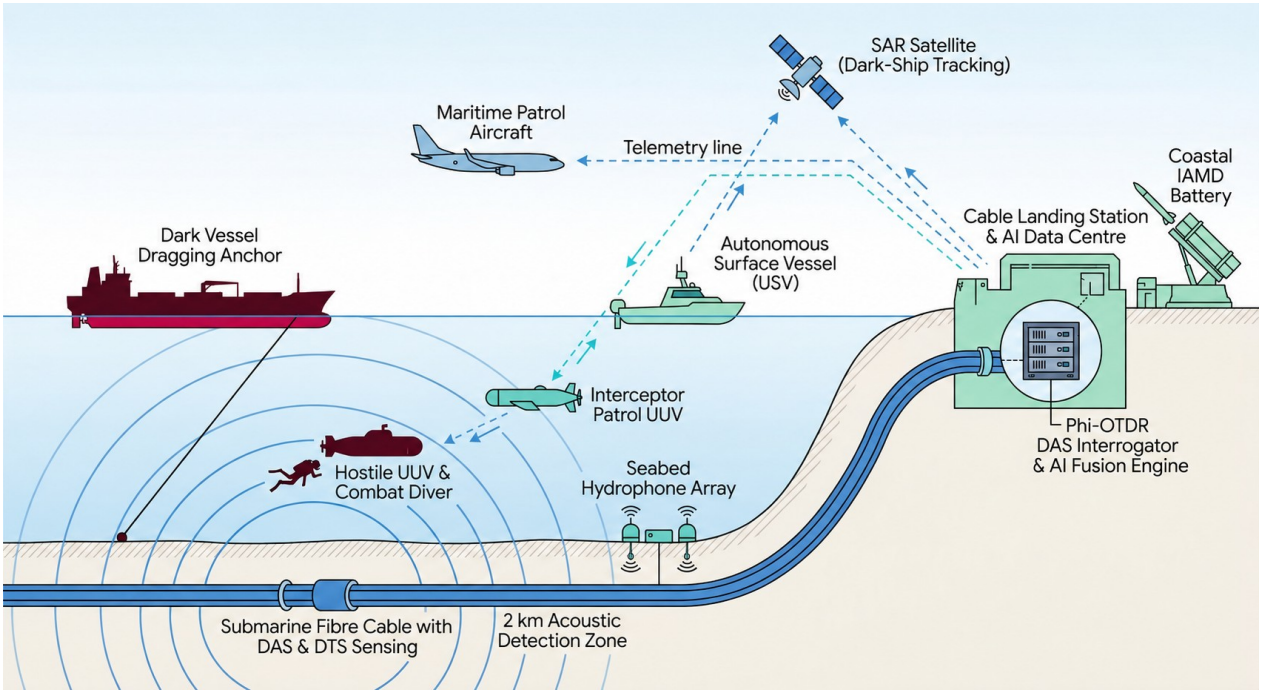
In a wider conflict, the IRGC could bypass the seabed altogether by using drones, cruise missiles and ballistic missiles, or cyberattacks, against coastal cable landing stations (CLS) and adjacent hyperscale data centres. Cables are particularly exposed where they come ashore and connect to terrestrial backhaul networks linking landing stations, cities and data centres. Potential threats include ballistic and cruise missiles and one-way attack drones. Iran's arsenal includes solid- and

liquid-fuelled ballistic missiles, among them the single-stage, solid-fuelled Fateh-110-D with a range of 300 kilometres, the Qiam-1 with a range of 1,500 kilometres, the Ghadr-110 with a range of 1,800–2,000 kilometres and the long-range, solid-fuelled Sejjil-2. It also includes domestically produced long-range land-attack cruise missiles such as Soumar and Hoveyzeh, alongside one-way attack drones. Disabling operations does not require the physical destruction of an entire data centre. Hyperscale AI facilities depend on the intersection of very high electricity consumption and scarce desalinated water for cooling. Attacks on nearby substations, cooling-water intakes or cable landing station power supplies, or coordinated cyberattacks against Border Gateway Protocol (BGP) routing and industrial networks, can therefore disrupt cloud and AI computing clusters, depending on their protection and redundancy.

A layered framework for cable protection

Moving from vulnerability assessment to effective defence requires improved surveillance of maritime corridors and the integration of sensor data to reduce detection gaps. Protecting submarine cables and coastal data infrastructure calls for a layered system that combines military engineering with geopolitical considerations, integrating fibre-optic sensing, autonomous maritime robotics, physical protection, coalition naval patrols and deterrence across multiple domains.

Figure 2. Integrating sensing, surveillance and protection at cable landing stations



Technical and physical protection and intelligent monitoring

Fibre-optic sensing allows some submarine cables to monitor surrounding vibrations continuously. An important technological development in the protection of subsea infrastructure is the ability to turn the cables themselves into continuously operating, real-time "sonar" arrays. By connecting a distributed acoustic sensing (DAS) interrogator, such as Hawk Measurement Systems' Praetorian or AP Sensing's FIBERMARS, to spare dark fibre or a dedicated wavelength channel within an onshore cable landing station, operators can monitor tens of kilometres of seabed continuously without deploying powered electronic equipment underwater.

DAS operates through phase-sensitive optical time-domain reflectometry (ϕ-OTDR), which measures changes over time in light backscattered

along the fibre, combined with optical pulse-compression reflectometry. An onshore interrogator injects highly coherent, narrow-linewidth laser pulses into the fibre core, where microscopic variations in the refractive index produce Rayleigh scattering. Acoustic waves or mechanical vibrations in the surrounding water or seabed sediment cause minute changes in the fibre's strain, altering the amplitude and phase of the backscattered light. Such disturbances include low-frequency cavitation associated with ships' engines and propellers, caused by the formation and collapse of bubbles; the acoustic signature of a UUV's propulsion system; disturbance from a combat diver; or mechanical changes as an anchor strikes and drags along the seabed.

Controlled maritime trials have demonstrated that DAS can track an individual diver along a cable and identify the precise location of underwater activity, for example at the 400-metre mark. Complementary techniques, including distributed temperature sensing (DTS), high-loss loopback (HLLB) interferometry and state-of-polarisation (SOP) monitoring, can detect abnormal thermal changes and mechanical strain over very long repeatered submarine cable routes.

Deploying DAS across the Arabian Gulf presents a substantial data-management challenge. A single submarine cable interrogator can generate up to one petabyte of raw acoustic data each day, depending on measurement settings and sampling rates. Early applications that relied solely on image-classification algorithms to identify a vessel's wake directly above the fibre are inadequate for proactive protection, which requires detecting threatening vessels well before they reach the cable. Telecommunications operators and defence ministries can address both challenges by developing automated machine-learning (ML) processing pipelines, using the 2026 Marlinks-NS DAS North Sea benchmark dataset for training and testing. The dataset contains 74,771 labelled samples across 250 sensing channels over a 2,554-metre section of a buried, 28-kilometre submarine cable. ML-based systems perform two complementary tasks in real time. Binary classification filters ambient noise, including whales, drifting containers and currents, and determines whether a vessel has crossed a critical proximity threshold. A regression model, which estimates numerical values, then assesses the lateral distance and direction of approach between the cable and the nearest vessel. These models require local validation before their outputs are adopted for operational warning.

Integrated AI-enabled seabed surveillance

Although DAS provides continuous localisation along a cable regardless of weather conditions and without requiring transponders aboard cooperating vessels, effective interception requires its outputs to be integrated into a wider, multi-domain intelligence architecture. AIS data provide a reliable basis for classifying cooperative surface vessels, while identifying non-cooperative ships or submerged targets requires corroboration across multiple sensors. In an integrated Gulf architecture, the onshore DAS machine-learning engine would feed a central AI-enabled data-fusion platform alongside fixed seabed hydrophone arrays, coastal radar, AIS data and synthetic aperture radar (SAR) imagery supplied by national operators such as the UAE's Space42. When a regression model detects an acoustic track approaching a warning zone extending two kilometres from the cable, the fusion engine would correlate its position with AIS data and SAR imagery. A surface vessel slowing to a speed consistent with anchor dragging while disabling AIS, entering "dark-ship" mode or transmitting false coordinates would trigger an alert. So would an underwater acoustic track approaching the cable without a corresponding surface radar return, potentially indicating a Ghadir-class midget submarine, a UUV or a swimmer delivery vehicle. The system would then direct uncrewed surface vessels (USVs), interception UUVs and maritime patrol aircraft (MPAs) towards the identified coordinates before the target reaches the cable.

Physical protection of submarine cables and coastal connections

Alongside active sensing networks, physical engineering measures should increase the energy required to sever a link or disable a coastal node. In the shallow waters of the Arabian Gulf and Hormuz, at depths of 35–90 metres, newly installed and replacement cable sections should use double galvanised-steel wire armouring covered by high-density polyethylene (HDPE). Where cables cross hard carbonate outcrops or existing oil and gas pipelines, operators should provide additional protection through graded rock placement, split cast-iron pipes or concrete mattresses against anchor dragging and shaped explosive charges. In soft sediment and dredged shipping channels, conventional plough burial to a depth of one metre offers insufficient protection from the multi-tonne anchors of very large tankers. High-pressure water-jet trenching should therefore support burial at depths of 3–5 metres or more, reaching 20–25 metres beneath busy navigation channels, while DAS algorithms are calibrated for changes in seabed conditions and the effect of greater depth on acoustic coupling.

The exposure of unprotected digital infrastructure ashore also reveals the limits of assuming that national air defences will automatically protect commercial cloud facilities. Gulf states should include cable landing stations, data centres and computing campuses among their critical infrastructure protection priorities: a data centre's reliability rating is not a rating of its protection against attack. They should assess the need for dedicated short- and medium-range integrated air and missile defence (IAMD) at major cable landing stations in locations such as Fujairah, Kalba, Barka, Dubai, Doha, Manama, Dammam and Kuwait, and at AI computing campuses including Stargate UAE and Khazna. Relevant capabilities may combine physical counter-drone interception, high-energy lasers and electronic warfare jamming. New cable landing projects should also replace the concentration of coastal equipment in a single building with distributed, blast-resistant underground beach manholes, from which fibre pairs connect to multiple geographically dispersed inland terminals. These terminals should have independent closed-loop water-cooling systems and microgrid power-generation capacity.

Maritime and legal frameworks

Securing maritime corridors requires coordination among defence authorities, coastguards and cable operators. Relevant GCC institutions could examine a permanent force or coordination mechanism for protecting subsea infrastructure in cooperation with the Bahrain-based Combined Maritime Forces (CMF), particularly Combined Task Force 152 (CTF 152). This multinational coalition is responsible for maritime security in the Arabian Gulf, with its command rotating among GCC naval and coastguard forces, including those of Kuwait, Saudi Arabia and the UAE. It already provides an established operational framework through Operation Sea Shield and annual activities such as Stakenet and maritime infrastructure protection exercises (MIPEX). Participants include Kuwait's navy and coastguard, the US Navy and Coast Guard, the Qatari navy, the Royal Bahrain Naval Force, the UAE Navy, British Royal Navy mine-countermeasure vessels and the Royal Saudi Naval Forces. Saudi Arabia's Eastern Fleet at Jubail is undergoing a wider modernisation under Project Tuwaiq, incorporating Saud-class multi-mission surface combatants, Al Riyadh- and Al Madinah-class frigates and Al Jubail-class Avante 2200 corvettes equipped with the indigenous HAZEM combat management system. Formally extending CTF 152's mandate beyond surface oil and gas installations to continuous protection of critical underwater infrastructure (CUI), and integrating seabed-protection technologies developed by AUKUS and tested by British, US and Australian naval forces in July 2026, could enable the coalition to establish no-anchor subsea infrastructure protection zones over cable routes in Hormuz.

This effort also requires real-time intelligence sharing among relevant defence ministries, regional telecommunications operators, including e& and its submarine cable subsidiary E-marine,

stc, Ooredoo, Batelco/Beyon, Omantel and Zain, and US and domestic hyperscale cloud providers, including Microsoft Azure, AWS, Google Cloud, Meta and G42.

A permanent subsea intelligence-fusion cell would allow commercial network operations centres to transmit DAS acoustic alerts and optical power-loss measurements directly to CTF 152 and national maritime operations centres. In structuring this public–private partnership, GCC governments should observe the ICPC policy framework of 16 February 2026 on fibre-optic sensing in submarine cables. Given the technology's dual-use character, the Committee calls for regulatory restraint: collaboration with industry experts rather than costly obligations that exceed technical maturity; recognition that commercial telecommunications cables exist to transmit data across the seas, rather than solely to monitor the marine environment; protection against coastal states' jurisdictional expansion that undermines cable freedoms under the United Nations Convention on the Law of the Sea (UNCLOS); and avoidance of embedded sensors that impair optical transmission. By funding and operating passive onshore DAS interrogators within sovereign cable landing stations, while leaving offshore infrastructure in international waters untouched, GCC states can improve seabed situational awareness without compromising the safeguards of the law of the sea.

Technical protection should be reinforced by a declared doctrine of deterrence across multiple domains, combining punishment with interdependent interests. First, the GCC and the United States should announce a joint policy under which covert UUV sabotage, limpet-mine attacks or deliberate shadow-fleet anchor dragging against Gulf cables or data centres would undergo a security and legal assessment of severity, responsibility and appropriate response options. This requires graduated responses determined by competent authorities after establishing attribution and assessing necessity, proportionality and civilian consequences under international law. Technical alerts alone should not trigger an automatic military response. Second, Gulf diplomacy should systematically draw on the risk of damage rebounding on the attacker. Iran's own connectivity uses the Oman–Iran link and FALCON, while Chinese and Indian state telecommunications companies, including China Mobile, China Unicom and Tata Communications, and commercial supply chains depend heavily on AAE-1, SEA-ME-WE 5, 2Africa and TGN-Gulf. Gulf foreign ministries should therefore establish joint institutional mechanisms with Beijing and New Delhi for digital infrastructure security. Coordination with China and India may raise the diplomatic cost of disrupting connectivity, without assuming identical interests or a guaranteed response.

Connectivity alternatives in the event of cable disruption

Even the strongest deterrence arrangements may be tested if regional hostilities escalate into a wider confrontation. If the Islamic Revolutionary Guard Corps (IRGC) carries out a coordinated campaign that severs all submarine cables crossing the Strait of Hormuz, GCC states must immediately activate a four-pillar system of alternatives. This system would bypass the maritime chokepoint, reroute intercontinental data traffic overland, sustain priority communications through space-based networks and maintain domestic economic activity by operating sovereign cloud services independently when external connectivity is lost, an approach known as digital islanding.

Option 1: maritime routes outside Hormuz

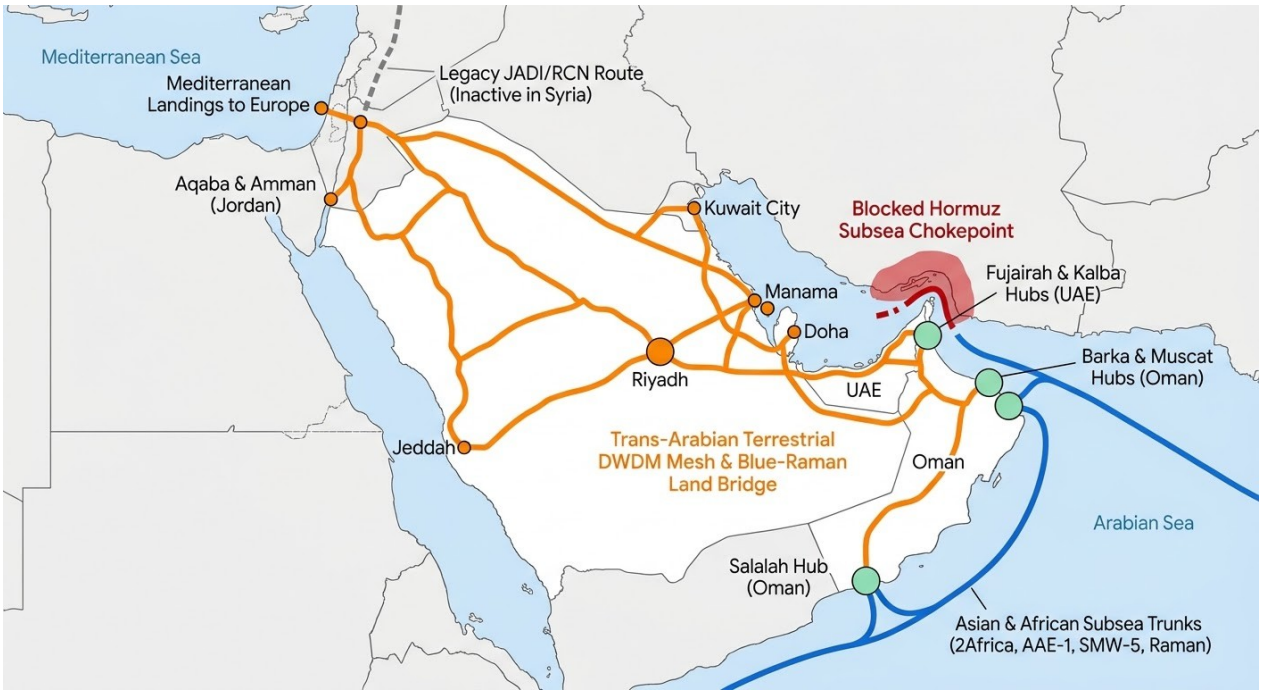
The GCC's greatest single geographical advantage is the Arabian Peninsula's direct access to deep water in the Gulf of Oman and the Arabian Sea, entirely outside the Strait of Hormuz's narrow

corridor. Over the past two decades, the UAE and Oman have strategically developed major clusters of cable landing stations on their eastern and southern coasts. Intercontinental cables terminate at these sites before reaching the strait.

Along the UAE's eastern coast on the Gulf of Oman, particularly Fujairah, Khor Fakkan and Kalba, 70–100 kilometres south of the Strait of Hormuz, e& and international consortia operate the Arabian Gulf region's largest submarine cable hub. Numerous regional and intercontinental systems, including SEA-ME-WE 3, SEA-ME-WE 4, SEA-ME-WE 5, AAE-1, 2Africa, Europe India Gateway (EIG), TGN-Gulf, GBI, FALCON, TEAMS and PEACE, land directly at Fujairah or Kalba without passing through Hormuz. Further south along the Gulf of Oman and Arabian Sea, Oman has established landing hubs at Barka, Muscat (Seeb), Duqm and Salalah. These deep-water locations lie beyond the reach of IRGC coastal artillery and shallow-water mining operations in Hormuz. Systems such as 2Africa, Blue–Raman's Raman segment, AAE-1 and SEA-ME-WE 5 terminate directly at Barka, Muscat or Salalah.

Disruption to submarine segments crossing Hormuz therefore does not necessarily disconnect the UAE or Oman from the global internet, or interrupt the main Asia–Europe trunks of systems such as AAE-1, whose intercontinental route bypasses the inner Gulf. The strategic challenge instead shifts from maritime access to terrestrial backhaul capacity: how effectively can hundreds of terabits per second of international traffic arriving at Fujairah, Kalba, Barka and Salalah be carried overland, across the Hajar Mountains and Arabian desert, to Abu Dhabi, Dubai, Doha, Manama, Riyadh and Kuwait City?

Figure 3. Alternative maritime gateways and terrestrial links



Option 2: terrestrial fibre corridors across the Arabian Peninsula

Terrestrial fibre networks across the Arabian Peninsula are the only transmission medium capable of matching submarine cables' multi-terabit throughput and low latency. Between 2010 and 2012, regional telecommunications operators sought alternatives through two major projects designed to bypass maritime chokepoints. The first was JADI, the Jeddah–Amman–Damascus–Istanbul route, a 2,530-kilometre terrestrial fibre link developed by stc, Jordan Telecom, the Syrian Telecommunications Establishment and Türk Telekom. It comprised 920 kilometres in Saudi Arabia (36.4%), 770 in Jordan (30.4%), 480 in Syria (19.0%) and 360 in Türkiye (14.2%). The second, the Regional Cable Network

(RCN), was a 7,750-kilometre terrestrial ring using dense wavelength-division multiplexing (DWDM), connecting Fujairah, Riyadh, Amman, Damascus and Istanbul. The Syrian conflict, however, put the Syrian sections of both JADI and RCN out of service. Europe–Persia Express Gateway (EPEG), which crossed Iran overland, would also be unusable in hostilities with Tehran.

To bypass the inactive Syrian transit route and protect Europe–Asia traffic against risks associated with Hormuz and the Red Sea, GCC telecommunications companies and global hyperscale cloud providers have developed infrastructure based on land bridges across the Arabian Peninsula. Blue–Raman, developed in partnership by Google, Telecom Italia Sparkle, Omantel, stc and Zain Jordan, is a central component of this strategy. Instead of passing through Hormuz or Bab al-Mandab, the eastern Raman cable reaches Oman at Barka and Salalah, then extends through terrestrial fibre networks in Oman and Saudi Arabia to Aqaba in Jordan. There it connects to the Blue submarine system serving Greece, Italy and France. Regionally, a terrestrial fibre mesh links Oman and the UAE, through Saudi Arabia, to Qatar, Bahrain, Kuwait and Jordan. Major technology companies have also begun routing northern Gulf traffic along terrestrial fibre cables laid beside Iraqi oil pipelines towards Türkiye and Europe.

Although terrestrial networks offer lower latency than circuitous maritime routes, their capacity remains severely constrained, as researchers at TeleGeography and APNIC highlighted in October 2026. A modern submarine cable such as 2Africa can support up to 180 terabits per second, whereas cross-border terrestrial links were historically designed for much lower capacities, initially expanding in increments of 200 gigabits per second before developing into multi-terabit rings. TeleGeography experts warn that existing terrestrial capacity may be insufficient to absorb all Gulf submarine traffic if every Hormuz cable is severed simultaneously. Countries such as Qatar and Bahrain would consequently face acute congestion unless dark fibre routes and C- and L-band optical transmission systems are activated and expanded across the Saudi land bridge.

Option 3: satellite communications

Satellite communications must be assessed by distinguishing their ability to support specific services from their ability to replace the data traffic carried by submarine cables. Available options vary by orbit, contracted capacity, latency, terminal availability and licensing. Table 2 compares these options as complementary elements of a continuity plan. Their performance must be measured locally before they are relied upon.

Table 2. Comparing submarine, terrestrial and satellite connectivity

Criterion	Submarine cables through Hormuz	External gateways and terrestrial links	LEO satellites	MEO / GEO satellites
Available capacity	High for international traffic; actual capacity depends on segments, equipment and contracts.	The main bulk-traffic alternative if backhaul is equipped and capacity reserved in advance.	Support specific services; capacity varies by coverage, gateways, users and contracts.	Dedicated or shared capacity by service; requires contracts and compatible terminals.
Latency	Varies with route length, transit points and congestion.	May fall on shorter routes; measure between the actual endpoints.	Usually lower than GEO; affected by gateways and terrestrial routing.	Varies between orbits; higher in GEO because of distance.
Cost	Suitable for large data volumes; varies by contract and capacity.	Includes transport, transit and local connectivity; compare actual offers.	Depends on equipment, service and priority; no fixed multiple of fibre costs should be assumed.	Depends on guaranteed capacity, coverage, terminals and service level.
Risks	Anchor damage, dredging and sabotage, alongside threats to landing stations.	Bypassing Hormuz requires independent routing; terrestrial, power and landing-station risks remain.	Avoids submarine cable cuts, but faces jamming, power and ground-gateway risks.	Avoids submarine cable cuts; jamming resistance and ground dependence vary by system.
Crisis activation	Traffic can use intact segments; repair depends on access and resources.	May be rapid if capacity is equipped, reserved and tested beforehand.	Requires ready terminals, licences, available capacity and an operating plan.	Requires advance terminal preparation, switching arrangements and service testing.
Best use	General internet traffic, cloud services and international transactions.	Carrying the largest feasible share of traffic diverted to independent alternatives.	Emergency, healthcare, remote-site and other priority communications.	Government, industrial and corporate communications according to coverage and service level.

The comparison illustrates a fundamental principle: satellite constellations cannot replace submarine fibre-optic cables. Subsea fibre carries more than 90%, and by some measures up to 99%, of intercontinental data, because satellite capacity is orders of magnitude lower, the cost per gigabyte is higher and spectrum constraints are stringent. Whereas a single submarine cable carries tens to hundreds of terabits per second, orbital geometry means that only a small proportion of a low Earth orbit (LEO) constellation, whether SpaceX's Starlink, Eutelsat OneWeb or Amazon Kuiper, is within line of sight of the Arabian Gulf at any moment. Available regional capacity depends on beam allocation, user numbers, gateways, terminals and contracts; no fixed ratio to Gulf submarine cable capacity can be assumed. Satellite networks are therefore structurally unable to replace the scale of consumer internet traffic, real-time synchronisation of very large databases across AWS and Microsoft Azure availability zones, or the data transfer requirements of training and inference workloads on G42's Condor Galaxy supercomputers, which offer 4–8 exaflops of computing performance.

Commercial LEO constellations also depend on local regulatory licences and ground gateways, unless traffic is routed entirely through optical inter-satellite laser links. They use shared Ku- and Ka-band radio spectrum that may be subject to military electronic warfare jamming during intense conflict. Diversifying operators and orbits reduces dependence on a single provider, but

capacity and service quality must still be tested under emergency conditions.

The indispensable role of non-terrestrial networks is to sustain critical state and industrial functions through multi-orbit satellite systems anchored in sovereign capabilities. Recognising this need, the UAE and Saudi Arabia have developed strong national space companies. In 2024, the UAE merged its leading satellite operator, Al Yah Satellite Communications Company (Yahsat), with G42's AI-enabled geospatial intelligence company, Bayanat, to form Space42. Saudi Arabia's Public Investment Fund (PIF) established Neo Space Group (NSG) to develop sovereign satellite communications and geospatial services. Integrating Space42 and NSG's sovereign geostationary orbit (GEO) and LEO capabilities with SES O3b mPOWER's high-capacity medium Earth orbit (MEO) beams and commercial LEO constellations such as Starlink and OneWeb into national emergency-response frameworks would give GCC states more diverse backup routes for their highest-priority functions, subject to capacity, power and jamming constraints. These functions include military command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR); supervisory control and data acquisition (SCADA) at oilfields and liquefied natural gas (LNG) facilities; aviation and maritime logistics hubs; central-bank SWIFT messaging; and essential government ministries.

Option 4: protecting national cloud operations

A substantial loss of international connectivity can disrupt the domestic economy and public administration, particularly where internal transactions depend on servers abroad. This dependence diminishes when critical services can exchange data, authenticate users, resolve domain names and run applications locally. Arrangements for domestic operation during an outage should therefore be established alongside checks on electricity, cooling, backups and staffing. The presence of a data centre within national borders does not, by itself, guarantee service continuity.

Independent domestic operation requires three technical foundations. First, telecommunications operators, banks, energy companies and e-government portals should exchange domestic traffic through national internet exchange points, with tests confirming that routes remain within the country. Second, reliable local domain name system (DNS) services must be available, together with continued management of national domains, authentication and digital certificates. Updated local copies of the root zone can be used under appropriate technical arrangements; this does not mean creating a replica of each of the 13 logical root servers. Applications must also be reviewed for dependence on external licensing and validation services, so that local connectivity does not remain available while the services themselves fail.

Third, domestic cloud and AI investments should be used to operate critical services locally. In the UAE, Microsoft and G42 announced a 200-megawatt data-centre expansion through Khazna Data Centers in November 2025, with commissioning due to begin before the end of 2026. On 6 July 2026, Inception42 also strengthened its Microsoft partnership to integrate the Catalyst platform with Microsoft Copilot tools, supporting the processing of sensitive government and corporate data within the UAE. These investments provide a foundation for local application operation, but do not alone demonstrate that banking clearing systems, energy networks and public services will continue during an outage. Each application's external dependencies, backups, identity services and licensing arrangements must be tested.

Crisis management and response scenarios

To translate protective engineering and bypass routes into operational readiness, GCC national security councils, military commands and telecommunications regulators should test three

escalating scenarios across three distinct phases: hours 0–24, days 2–7 and days 8–30 and beyond, while addressing constraints on maritime repair. These are planning assumptions, not firm predictions. Their effects depend on fault locations, reserve capacity, continued power supply and maintenance teams' ability to gain access.

Three escalating scenarios

Scenario 1: limited disruption with uncertain attribution

This scenario assumes that an oil tanker associated with the "shadow fleet" transits Hormuz amid rising diplomatic tension, reports a propulsion failure and drags its 15-tonne anchor for several kilometres across the shallow seabed at a depth of 50 metres. It severs FALCON and the AAE-1 branch to Qatar, narrowly missing GBI. Suspected parties may deny responsibility, so determining whether the damage was deliberate requires investigation.

During hours 0–24, the operations centre gathers signal-loss data and available acoustic alerts and compares them with vessel movements and surveillance imagery to identify the damage and its probable cause. Operators reroute traffic to intact cable segments and terrestrial links whose readiness has been demonstrated, monitoring congestion and service quality. Technical data alone do not authorise boarding or detaining a vessel; competent authorities determine the response according to evidence and legal jurisdiction. During days 2–7, capacity-sharing agreements are activated and arrangements for permits, insurance, a repair vessel and any necessary protection are completed. During days 8–30 and beyond, repair, testing and phased service restoration continue. Completion dates depend on sea conditions, the fault location and the availability of vessels and spare parts, rather than a predetermined timetable.

Scenario 2: widespread disruption through Hormuz

The second scenario assumes damage to several operational cable segments crossing Hormuz, alongside damage to some landing stations or data centres. It tests Gulf states' ability to cope with the simultaneous loss of multiple routes, without counting unfinished projects as available capacity or assuming that every regional system passes through the strait. The impact depends on each country's and operator's reliance on affected segments and on the independence of alternative routes.

During hours 0–24, service-continuity plans are activated and workloads transferred to intact facilities and routes in line with previous testing. Emergency communications, healthcare, energy, payments and government services receive priority, with licensed and contracted satellite services activated where required. Successful switching remains conditional on functioning electricity, cooling, internal connectivity and identity management. Neither the prevention of most damage by defensive systems nor automatic cloud failover should be assumed. During days 2–7, operators expand available terrestrial capacity and allocate resources according to service requirements and performance measurements, introducing temporary, publicly communicated congestion-management measures where necessary. During days 8–30 and beyond, priority shifts to securing access to faults, protecting maintenance crews and restoring the segments with the greatest service impact. Security and military decisions remain the responsibility of competent authorities, separate from network traffic management.

Scenario 3: simultaneous disruption in Hormuz and Bab al-Mandab

The third scenario assumes simultaneous failures in segments crossing Hormuz and others passing through the Red Sea, placing pressure on the Arabian Peninsula's eastern and western gateways. It tests a crisis extending beyond Gulf connectivity to Asia–Europe links. Not every fault

is assumed to result from a coordinated operation, nor are the same actors presumed responsible for all damage. Investigating causes remains separate from restoring service.

During hours 0–24, traffic is redirected to intact routes permitted under operating contracts, potentially including longer paths around Africa or across the Pacific and North America. The effects on latency and transaction completion are measured, without assuming a uniform capacity loss across countries and services. During days 2–7, gateways outside Hormuz and terrestrial links independent of affected segments are used, while satellite capacity is allocated to the highest-priority services. Blue–Raman should be counted as a Red Sea bypass only after the independence of the route actually used has been verified. During days 8–30 and beyond, feasible services continue operating domestically while repair, financing and maritime access are coordinated. China, India and other international actors may help facilitate access to protect their interests, but this remains a diplomatic possibility. Permits, insurance and access conditions may also prolong the crisis without further cable cuts, requiring alternative operation to be combined with negotiations that facilitate repair.

A forward programme for crisis readiness

To strengthen continuity and reduce the impact of disruption, Gulf defence ministries and telecommunications regulators should implement a coordinated policy roadmap across three time horizons, together with telecommunications companies and sovereign AI and cloud operators. Relevant regulators are the UAE's Telecommunications and Digital Government Regulatory Authority (TDRA), Saudi Arabia's Communications, Space and Technology Commission (CST), Qatar's Communications Regulatory Authority (CRA), the Telecommunications Regulatory Authorities (TRA) of Bahrain and Oman, and Kuwait's Communication and Information Technology Regulatory Authority (CITRA).

Immediate measures: the first six months

During the first six months, littoral states should reduce seabed surveillance gaps and shortcomings in coastal air defence. National telecommunications regulators and defence ministries should fund trials and installation of onshore distributed acoustic sensing (DAS) and distributed temperature sensing (DTS) interrogators on suitable fibres at landing stations serving Hormuz and the Arabian Gulf, using the appropriate technology for each measurement. Expansion should follow ICPC guidance on industry cooperation and assessment of technical and regulatory limitations. Machine-learning-classified acoustic alerts should feed a new GCC–CTF 152 subsea intelligence-fusion cell, correlating them with Space42 synthetic aperture radar imagery and automatic identification system (AIS) data to track vessels that are not transmitting location information. Defence ministries should simultaneously classify major coastal landing stations at Fujairah, Kalba, Barka, Salalah, Dubai, Doha, Manama, Dammam and Kuwait, and hyperscale cloud and AI campuses operated by AWS, Microsoft Azure, G42/Khazna, Stargate UAE and Humain–stc, as priorities for critical infrastructure protection. This includes assessing the need for counter-unmanned-aircraft systems and integrated air and missile defence at these sites. Central banks, major energy companies and telecommunications regulators should conduct mandatory "Strait Connectivity Outage" exercises to verify that digital systems can operate smoothly without external connectivity through local internet exchanges, such as UAE-IX and SHB-IX, and updated local DNS services. Multi-orbit satellite terminals for Space42, Neo Space Group, SES O3b mPOWER, Starlink and OneWeb should be licensed and deployed in advance at the highest-priority defence, SCADA, banking and logistics sites. Finally, the GCC should establish a sovereign war-risk indemnity and a CTF 152 armed naval escort protocol to improve E-marine repair

vessels' ability to deploy during grey-zone crises or military confrontation, subject to crew readiness, permits and safe operating conditions.

Medium-term measures: six to 24 months

Over six to 24 months, Arabian Gulf littoral states should remove terrestrial backhaul bottlenecks and consolidate deterrence across domains. Telecommunications regulators in Oman, the UAE, Saudi Arabia, Qatar, Bahrain, Kuwait and Jordan should harmonise cross-border transit rules, remove terrestrial cross-border charges that inflate transit costs and agree with operators to equip and test usable reserve capacity through C- and L-band DWDM systems. These rings should connect external maritime hubs at Salalah, Duqm, Barka, Fujairah and Kalba to all capitals inside the Gulf and then to independent routes towards Aqaba and the Mediterranean, once readiness and actual routing have been verified. At sea, competent defence and maritime authorities should coordinate with CTF 152 to assess no-anchor subsea infrastructure protection zones along Hormuz cable corridors, within their legal jurisdiction. They should apply appropriate, site-specific burial and armouring standards to new and repaired segments and deploy unmanned surface vehicles (USVs) and unmanned underwater vehicles (UUVs) for monitoring, verification and response within approved mandates. Diplomatically, the GCC should combine a clear public doctrine of subsea deterrence, warning Tehran that grey-zone or military cable sabotage will prompt a proportionate response across domains, with formal GCC–China–India dialogue on digital lifeline security. This dialogue should draw on the exposure of Asian commercial companies and state telecommunications operators using AAE-1, SEA-ME-WE 5, 2Africa and TGN-Gulf, with the aim of restraining IRGC escalation.

Long-term measures: two to five years

Over a strategic horizon of two to five years, the GCC should build lasting protection into its digital and maritime infrastructure. To address the global shortage of cable ships and the possibility that vessels cannot gain access during wartime, Gulf sovereign wealth funds, including Mubadala, ADQ, PIF and the Qatar Investment Authority (QIA), could consider jointly expanding E-marine's fleet. This may include two next-generation cable-laying and repair vessels with class III dynamic positioning (DP-III) and crew-protection equipment suited to assessed risks. The vessels would carry remotely operated underwater vehicles (ROVs) for deep trenching, armoured crew shelters and integrated counter-drone electronic warfare systems, with permanent bases at expanded depots in Fujairah, Khor Fakkan and Salalah outside Hormuz. Gulf telecommunications regulators should also require submarine cable projects after 2027 to use underground beach manholes branching into three routes feeding geographically dispersed, blast-resistant inland terminals. Northern Gulf networks should connect to diverse terrestrial fibre corridors along energy rights of way in Iraq and Türkiye. Combining Space42 and NSG sovereign satellite constellations, portable sovereign AI systems such as digital embassies and Greenshield, eastern maritime gateways outside Hormuz and a protected trans-Arabian terrestrial network could reduce the impact of pressure on international connectivity. Continuous testing and updating would remain essential.

Conclusion

Iran's October 2026 threats against submarine cables and cloud computing centres reveal a fundamental change in the risks facing Arabian Gulf security. Digital infrastructure is now the backbone of post-oil economies, financial markets, supply chains and sovereign AI systems. Hormuz's geography and shallow waters give Tehran scope to use hybrid and grey-zone instruments, from dormant munitions and midget submarines to shadow-fleet anchor dragging under plausible deniability, as well as kinetic and cyberattacks against landing stations and data centres. Yet this threat is constrained by the prospect of harm rebounding on Iran itself, given interlocking Asian and international interests and Iran's reliance on the same shared networks.

If digital infrastructure is attacked, cable maintenance will depend on cooperative arrangements and commercial contracts that specify coverage areas, vessels and available resources. Established frameworks include the Mediterranean Cable Maintenance Agreement (MECMA) and the South East Asia and Indian Ocean Cable Maintenance Agreement (SEAIOCMA), alongside other regional and commercial arrangements. These agreements do not make every vessel available for every fault in the Gulf. E-marine plays a regional role in cable installation and maintenance, but selecting an appropriate vessel requires scrutiny of the contract, vessel location, equipment and existing commitments. Cooperation with Oman can coordinate logistical support, maritime access and diplomatic engagement to facilitate repair within the relevant jurisdictions.

Repairing a severed submarine cable nevertheless requires time and specialised maritime equipment. A repair vessel must reach the fault coordinates, lower grapnels to recover the severed ends from the seabed, hoist them aboard and spend days splicing hair-thin optical fibres with microscopic precision. It then returns the repaired section to the seabed while holding position through class II dynamic positioning (DP-II) thrusters. Throughout this operation, whose duration depends on the fault and working and access conditions, an unarmed commercial cable ship operating stationary within the 21-nautical-mile-wide Strait of Hormuz is highly exposed to IRGC anti-ship missiles, one-way attack drones, fast attack craft and naval mines.

Effective repair capacity diminishes when faults occur simultaneously, insurance becomes unavailable or crew risks increase. Readiness planning should therefore reserve maintenance resources, distribute spare parts, streamline permits and establish financing and insurance arrangements before a crisis. GCC states could consider joint war-risk guarantees and escort arrangements where necessary, after assessing their costs and responsibilities. Crew safety must remain a condition for deployment, with alternatives if access proves impossible. Readiness is measured by teams' ability to deploy, reach the fault, repair it and restore service, rather than by the number of vessels listed on paper.

Countering coercion through digital chokepoints requires littoral states to move beyond reactive fault management towards integrated deterrence based on denying gains and reinforcing shared interests. Four parallel strands give this approach practical effect. First, improve subsea situational awareness by integrating AI-enabled DAS and DTS within the CTF 152 framework, while treating cable landing stations and major computing campuses as tier-one national defence infrastructure. Second, activate geographical alternatives through secure landing hubs on the Gulf of Oman and Arabian Sea, and expand terrestrial bridges across the Arabian Peninsula and Iraq to avoid dependence on a single strait or paralysis when Hormuz and Bab al-Mandab are disrupted together. Third, use sovereign multi-orbit satellite networks to sustain command-and-control and critical-sector communications, alongside digital islanding protocols and sovereign cloud arrangements that keep domestic economic activity and public services operating independently. Fourth, secure the logistical and legal readiness of repair vessels, separate service restoration from criminal investigation and institutionalise diplomacy with Asian and European partners, turning their dependence on Gulf bandwidth into political support for deterring escalation.

References

Ahmed, Mostafa. 2026. "What If: Iran Targeted Submarine Internet Cables in the Arabian Gulf?" *Al Habtoor Research Centre*. https://www.habtoorresearch.com/publications/ran-submarine-internet-cables-arabian-gulf/

Bashfield, Samuel, and Oscar Youlten. 2026. "Fibre Sensing: How Undersea Cables Learned to Listen." *The Interpreter*, Lowy Institute, October 14. https://www.lowyinstitute.org/the-interpreter/fibre-sensing-how-undersea-cables-learned-to-listen

Bochinger, Steve. 2026. "The Middle East's Space Sector: From Ambition to Strategic Maturity." *Constellations*, Kratos, January 18. https://www.kratosspace.com/constellations/articles/the-middle-east-space-sector-from-ambition-to-strategic-maturity

CENTCOM Citadel. 2025. "Operation Sea Shield, CTF 152 Strengthen Maritime Security in Strategic Waters." January 23. https://centcomcitadel.com/en_GB/articles/ssc/features/2025/01/23/feature-01

Combined Maritime Forces. 2015. "CTF-152 Hosts International Maritime Infrastructure Protection Exercise in the Gulf." January 27. https://combinedmaritimeforces.com/2015/01/27/ctf-152-hosts-international-maritime-infrastructure-protection-exercise-in-the-gulf/

Drapp, B., and M. Mildner. 2025. "Enhancing Coastal Critical Infrastructure Protection with Distributed Acoustic Sensing (DAS)." Technical paper presented at UDT 2025. AP Sensing GmbH. https://www.apsensing.com/media/1813/download/2025-03%20Enhancing%20Coastal%20Critical%20Infrastructure%20Protection%20with%20Distributed%20Acoustic%20Sensing%20-%20Drapp%20B._DAS_Critical_Infrastructure_Subsea_Cables.pdf?v=1

E-marine. n.d. "Projects." Accessed October 21, 2026. https://emarine.ae/en/Projects

ET Online. 2026. "Could Iran Target the Gulf's Digital Backbone? The Risks to Data Centres and Internet Cables Explained." *The Economic Times*, October 14. https://economictimes.indiatimes.com/news/international/world-news/could-iran-target-the-gulfs-digital-backbone-the-risks-to-data-centres-and-internet-cables-explained/articleshow/134925481.cms

Gelvanovska, Natalija, Michel Rogy, and Carlo Maria Rossotto. 2014. *Broadband Networks in the Middle East and North Africa: Accelerating High-Speed Internet Access*. Washington, DC: World Bank. https://doi.org/10.1596/978-1-4648-0112-9

Hawk Measurement Systems. n.d. "Fiber Optic Sensing for Subsea Cable Monitoring." Accessed October 21, 2026. https://www.hawkfiber.com/praetorian-fiber-optic-sensing-for-subsea-cable-monitoring/

International Cable Protection Committee (ICPC). 2026a. "As Fibre-Optic Sensing in Submarine Cables Develops Rapidly, Governments Should Exercise Restraint in Regulating." Updated February 16. https://www.iscpc.org/publications/icpc-viewpoints/as-fibreoptic-sensing-in-submarine-cables-develops-rapidly-governments-should-exercise-restraint-in-regulating/

International Cable Protection Committee (ICPC). 2026b. "Media Enquiries & Frequently Asked Questions." Updated May 20. Accessed October 21, 2026. https://www.iscpc.org/news/media-enquiries/

International Telecommunication Union. 2012. *Background Paper on Access and Infrastructure.* Connect Arab Summit, Doha, March 5–7. Prepared February 15. https://www.itu.int/net4/ITU-D/CDS/gq/generic/asp-reference/file_download.asp?FileID=574

International Telecommunication Union. 2026. *International Advisory Body on Submarine Cable Resilience: Report of the Working Groups.* Geneva: International Telecommunication Union. https://www.itu.int/digital-resilience/submarine-cables/wp-content/uploads/sites/2/2026/07/IAB-Publication-2026.pdf

Jain, Shweta. 2026. "G42 and Microsoft Deepen Partnership to Keep Sensitive AI Data inside the UAE." *The National*, July 6. https://www.thenationalnews.com/future/technology/2026/07/06/g42-and-microsoft-deepen-partnership-to-keep-sensitive-ai-data-inside-the-uae/

Koley, Bikash. 2021. "Announcing the Blue and Raman Subsea Cable Systems." *Google Cloud Blog*, July 29. https://cloud.google.com/blog/products/infrastructure/announcing-the-blue-and-raman-subsea-cable-systems

Kumari, Warren, and Paul Hoffman. 2020. *Running a Root Server Local to a Resolver*. RFC 8806. Internet Engineering Task Force, June. https://www.rfc-editor.org/rfc/rfc8806.html

Lambert, Guillaume. 2026. "Hormuz, Act II: When Iran Simultaneously Threatens Ships and Submarine Cables." Aevum Advisory, May 26. https://www.aevum-advisory.com/en/hormuz-act-ii-when-iran-simultaneously-threatens-ships-and-submarine-cables/

Microsoft. 2025. "Microsoft and G42 Accelerate UAE's Digital Future with Major Data Centre Expansion." *Source EMEA*, November. https://news.microsoft.com/source/emea/2025/11/microsoft-and-g42-accelerate-uaes-digital-future-with-major-data-centre-expansion/

O'Neill, Tim. 2026. "Turning the Seabed into a Sensor: The Future of Critical Infrastructure Protection." BAE Systems, October 2. https://www.baesystems.com/en-uk/insight/turning-the-seabed-into-a-sensor-the-future-of-critical-infrastructure-protection

Ramirez-Torres, Erick Eduardo, Javier Macias-Guarasa, Daniel Pizarro, Javier Tejedor, Sira Elena Palazuelos-Cagigas, Pedro J. Vidal-Moreno, María R. Fernández-Ruiz, Sonia Martin-Lopez, Miguel Gonzalez-Herraez, and Roel Vanthillo. 2026. "A Distributed Acoustic Sensing Dataset for Vessel Detection and Localization in Submarine Cable Protection." Preprint, arXiv, July 31. https://doi.org/10.48550/arXiv.2607.28306

TeleGeography. n.d. "Submarine Cable Map." Accessed October 21, 2026. https://www.submarinecablemap.com/