What If: Iran Targeted Submarine Internet Cables in the Arabian Gulf?

April 2026

AL HABTOOR RESEARCH CENTRE

Strategic Estimates

The contemporary global economy is anchored in a tightly integrated digital and physical infrastructure, in which the continuity of international markets depends on an extensive network of submarine fibre-optic cables spanning approximately 1.3 million kilometres. This strategic architecture carries between 95 and 99% of intercontinental digital communications and constitutes the foundational layer for the settlement of daily financial transactions valued at roughly 10 trillion dollars. For decades, geopolitical analysis has prioritised the security of surface maritime corridors to safeguard the uninterrupted flow of conventional energy resources. Yet evolving realities indicate a decisive shift. The durability of the global economic system now hinges just as critically on protecting these submerged networks, which have emerged as indispensable arteries of global connectivity and financial stability.
This reality is especially visible in the Middle East, particularly across the Arabian Gulf, the Strait of Hormuz, the Arabian Sea, and the Red Sea, where the geographic corridors that govern trade flows and energy supply chains overlap with the main routes of global data transmission. The Strait of Hormuz, which is only 21 nautical miles wide, sits at the centre of this convergence. Around 21 million barrels of crude oil and one-third of global liquefied natural gas supplies pass through it each day. At the same time, 17 submarine cable systems run across its seabed, carrying nearly 30% of total international internet traffic. This intense concentration of physical and digital infrastructure within a narrow geographic space creates a severe security vulnerability. It exposes the global economy to systemic risks tied directly to regional instability.

These structural risks moved from theoretical assessment to operational reality with the outbreak of direct military confrontation in early 2026 between the United States and Israel on one side and Iran on the other, in what became known as Operation Epic Fury. These developments marked a fundamental shift in Iranian military doctrine. Faced with growing limits on its ability to disrupt surface energy flows through conventional means, Iran increasingly turned toward asymmetric threats. This shift is reflected in a move away from the traditional threat of closing maritime chokepoints to the deliberate targeting of submarine internet cable networks, using their disruption as a tool of deterrence and geopolitical pressure. It represents a calculated effort to exploit the physical vulnerabilities of civilian infrastructure to offset conventional power imbalances. In doing so, it introduces risks that extend well beyond the regional theatre and directly affect the foundations of the digital economy, in an era increasingly shaped by hybrid warfare and the militarisation of the maritime domain.

This emerging pattern of threat also creates what can be classified academically as a dual and simultaneous crisis. In such a scenario, the systematic disruption of submarine cables would paralyse global energy supply chains while simultaneously causing severe degradation across the digital infrastructure of the Middle East, South Asia, and Europe.

The immediate consequences would extend far beyond the loss of communications services for individuals. They would include major disruptions to electronic clearing systems that underpin sovereign wealth fund investments, as well as the paralysis of digital command-and-control centres operated by state-owned energy conglomerates. Such targeting would also disrupt military command-and-control networks and sever the communication channels needed to manage maritime navigation and to reroute vessels during crises. It would further undermine the artificial intelligence and cloud computing infrastructure on which many states in the region rely for their economic diversification strategies.

The plausibility of these threats is reinforced by recent material precedents that have exposed the infrastructure's real vulnerabilities. Most notable was the damage inflicted on Red Sea cable systems following the sinking of the Rubymar in 2024, followed by multiple line disruptions in the same region in September 2025. Together, these incidents underscore the fragility of these networks in the face of both accidental disruptions and deliberate acts of sabotage.

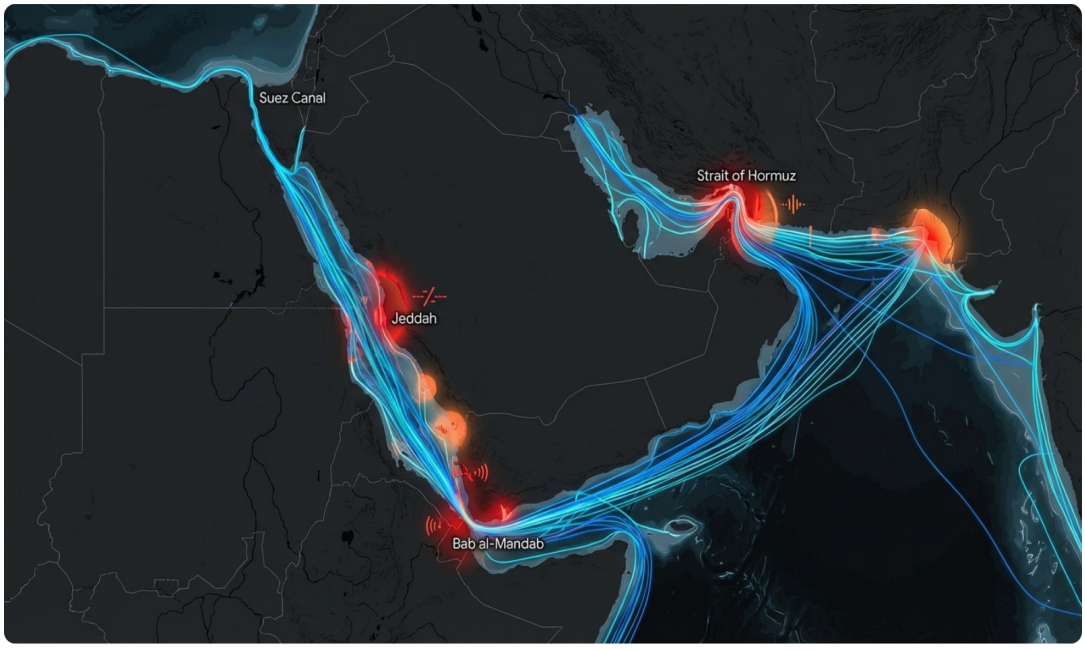
Building on these complex strategic and economic dynamics, this paper examines the implications of a large-scale attack targeting submarine communications infrastructure in the Arabian Gulf. It does so through a detailed assessment of the technical and military capabilities available to Iran to carry out physical sabotage operations beneath the seabed, alongside an analysis of the strategic motives driving this form of asymmetric escalation. By integrating recent historical precedents with updated data on regional and international levels of digital dependence, the paper seeks to assess the scale of the losses likely to result should such a scenario materialise.

I. The Geopolitics of Submarine Cables in the Arabian Gulf

Strict geographical constraints shape the physical infrastructure underpinning global communications networks. Natural topography forces intercontinental data routes to converge within a limited number of maritime corridors that function as strategic chokepoints. In the Middle Eastern context, the route extending from the Mediterranean Sea through the Suez Canal and the Red Sea, and onward to the Gulf of Aden, the Arabian Sea, and the Arabian Gulf, forms the central geostrategic axis linking advanced European economies and emerging African markets with the major population centres of the Indian subcontinent and Southeast Asia.

These structural constraints are most acute in the Strait of Hormuz, where topographical limits are particularly severe. At its narrowest point, the strait measures just 21 nautical miles, with commercial shipping lanes restricted to only two miles in each direction. This spatial pressure is intensified by ongoing security and political tensions involving Iran, leading network operators to concentrate most submarine cable routes within the confined corridor of Omani territorial waters. This excessive clustering of digital infrastructure within a highly restricted space creates a critical physical vulnerability. Even a routine maritime incident, such as the accidental dragging of an anchor by a large commercial vessel, or a deliberate act of sabotage, could disrupt multiple independent international communication systems at once. Such disruption would carry immediate consequences for the global digital economy and heighten systemic instability.

Figure (1): Chokepoints in Subsea Infrastructure in the Middle East



These transcontinental routes are complemented by regional systems built on resilient ring architectures, such as the Falcon and Transworld networks, which help preserve connectivity across the Gulf Cooperation Council states and the Indian subcontinent. They are further reinforced by low-latency links, including the Europe India Gateway and Asia-Africa-Europe cable systems, which are designed to minimise transmission delays.

The development of this infrastructure is also deeply shaped by geoeconomic competition. The expansion of projects such as the PEACE cable reflects China's growing technological footprint in the region and its effort to secure routes aligned with Beijing's strategic ambitions. Yet future expansion plans face major operational constraints in an increasingly volatile security environment. This became clear when the companies behind the Africa-2 submarine cable project, which intended to establish one of the world's longest connectivity systems, were forced to suspend deployment activities and invoke force majeure clauses following the escalation of military tensions in Gulf waters. This episode underscores how closely the development of digital infrastructure remains tied to regional security conditions.

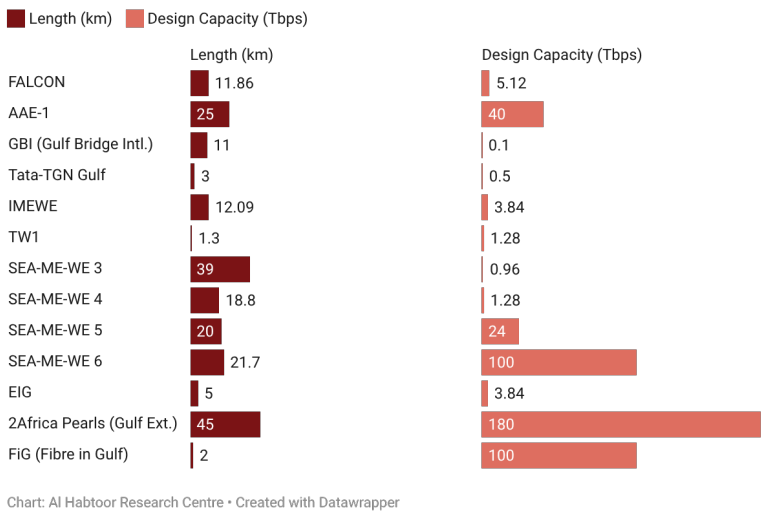
Table (1): Distribution of Major Submarine Cable Systems in the Arabian Gulf

Cable System	Key Landing Points in the Gulf	Routing Corridor
FALCON	Extends across the Arabian Gulf with landing points in Kuwait, Bahrain, Qatar, Saudi Arabia, the UAE, Iran, and Oman	Hormuz / Gulf
AAE-1	Fujairah (UAE), Oman	Gulf of Oman
GB (Gulf Bridge Int.)	UAE, Qatar, Bahrain, Kuwait, Saudi Arabia, Oman	Hormuz
Tata TGN Gulf	UAE, Qatar, Bahrain, Saudi Arabia, Oman	Hormuz
IMEWE	Kuwait, Bahrain, UAE, Saudi Arabia	Hormuz
TW1	UAE (Fujairah), Oman	Arabian Sea
SEA-ME-WE 3	Jeddah (Saudi Arabia), Fujairah (UAE), Karachi (Pakistan)	Red Sea
SEA-ME-WE 4	Jeddah (Saudi Arabia), Fujairah (UAE), Karachi (Pakistan)	Red Sea
SEA-ME-WE 5	Jeddah (Saudi Arabia), Fujairah (UAE), Karachi (Pakistan)	Red Sea
SEA-ME-WE 6	Jeddah (Saudi Arabia), Fujairah (UAE), Karachi (Pakistan)	Red Sea
EIG	Oman, UAE, Saudi Arabia	Red Sea
2Africa Pearls (Gulf Ext.)	Dammam (Saudi Arabia), multiple GCC locations	Hormuz
FIG (Fibre in Gulf)	UAE, Qatar, Bahrain, Kuwait, Oman, Iraq	Gulf Edge

The vulnerabilities embedded in these critical networks extend well beyond their surface-level geographic concentration. They also stem from the hydrographic characteristics of the marine environment and from the final distribution of data at coastal landing points. The waters of the Arabian Gulf are exceptionally shallow, with an average depth of no more than 50 metres. This deprives submerged cables of the natural protection afforded by deep-ocean basins and leaves them exposed to physical interference from conventional military equipment, unmanned underwater vehicles, or even commercial diving teams. This weakness is compounded by the extreme concentration of data landing hubs. The overwhelming majority of cable systems crossing the Arabian Sea converge within a narrow coastal strip in Mumbai, concentrated along a stretch of roughly 6 kilometres at Versova Beach. This single corridor alone handles nearly 95% of India's international bandwidth capacity.

The severity of this vulnerability is further amplified by a sharp regional shortfall in specialised maintenance logistics. Key states such as India lack dedicated cable repair vessels and remain fully dependent on foreign contractors based in hubs such as Dubai and Singapore. In active conflict environments, civilian repair ships are unlikely to operate without full military protection and exceptional insurance coverage, given the risks posed by anti-ship threats. As a result, routine faults can quickly escalate into prolonged outages lasting for months. This risk is further intensified by the growing subsea presence of advanced assets operated by major powers, including submarines and intelligence-gathering research vessels capable of precise physical interference or covert surveillance, while maintaining plausible deniability. In this context, a coordinated attack targeting the routes that pass through the Strait of Hormuz and the landing points in the Arabian Sea emerges as a credible scenario with the potential to impose a highly effective digital blockade.

Figure (2): Technical Specifications of Submarine Cable Networks in the Arabian Gulf



As part of a strategic effort to reduce reliance on submarine cables and limit their security exposure, states across the region have intensified investment in alternative routing options based on terrestrial fibre-optic networks. These initiatives seek to redirect data flows overland toward Asian and European markets and to establish integrated connectivity systems.

Regional connectivity relies on an advanced terrestrial infrastructure, most notably the Middle East Electricity Transmission System (MEETS), a 1,400-kilometre network built on fibre-optic lines integrated into the Gulf Cooperation Council Interconnection Authority's electricity transmission grid. This system provides direct connectivity between the United Arab Emirates, Qatar, Bahrain, Saudi Arabia, and Kuwait. This backbone is complemented by the Regional Cable Network (RCN), which extends approximately 5,000 kilometres from Fujairah through Riyadh to Amman, with an initial transmission capacity of 1.2 terabits per second. To further strengthen resilience, the JADI network supports this architecture by providing additional routing capacity toward northern corridors.

Despite the added value of these terrestrial alternatives, particularly in geographic diversification and lower data latency, technical and geopolitical assessments reveal deep structural limits that prevent them from serving as a comprehensive substitute for submarine systems. The central technical constraint is that land-based cables cannot match the vast capacity of modern subsea networks. As a result, they are unable to absorb and reroute the full volume of international digital traffic in the event of a large-scale maritime disruption. These overland routes also face security and regulatory challenges comparable to those found in the maritime domain. Their passage through regions marked by political instability, armed conflict, and sharp economic disparities, particularly across the Levant, exposes them to persistent risks of physical sabotage. Consequently, the stability of both the regional and global digital economy remains fundamentally tied to the integrity of critical maritime corridors.

II. The Evolution of Strategies Targeting Maritime Infrastructure

The targeting of critical infrastructure in the maritime domain represents a systematic extension of military doctrines that have historically sought to control the flow of information and resources through strategic geographic corridors. These practices are rooted in earlier international conflicts, where the deliberate disruption of communication lines emerged as a central tactic for weakening an adversary's operational capacity. This pattern can be traced from US military operations against Spain in the late nineteenth century to direct British intervention during the First World War, when submarine telegraph cables were severed in order to consolidate control over the global information environment.

In the Middle Eastern context, maritime confrontations during the Iran–Iraq War between 1984 and 1988, particularly during what became known as the Tanker War, marked a formative stage in the use of maritime corridors as instruments of geopolitical pressure. At that time, operations focused on disrupting surface energy transport routes using naval mines and fast-attack craft. With the deeper shift toward a digitalised global economy, this military logic has evolved from targeting physical assets tied to traditional supply chains to targeting the submerged infrastructure responsible for data transmission. This progression confirms that the strategic use of maritime corridors to impair an adversary's capabilities remains a highly adaptable approach, one that continues to evolve in line with prevailing technological and economic conditions.

The potential effectiveness of this contemporary strategic threat rests on a clear understanding of the inherent structural fragility of submarine cable systems. These vulnerabilities were exposed long before they entered the logic of deliberate military targeting, having already been revealed by a series of natural disasters and accidental disruptions.

Natural disasters have repeatedly exposed the severe lack of structural resilience and redundancy across certain corridors. This was evident in the disruption that paralysed banking and digital services across Southeast Asia following the 2006 Hengchun earthquake in Taiwan, and in the complete isolation imposed on Tonga in 2022 after a volcanic eruption severed the country's only international connectivity link.

These structural vulnerabilities also intersect with incidents caused by unintentional human activity or limited material motives. A notable example was the simultaneous cable disruptions in the Mediterranean basin and the Arabian Gulf in early 2008, when commercial vessels dragged their anchors while attempting to avoid adverse weather. That incident reduced regional network capacity by nearly 70 percent and disconnected tens of millions of users. These precedents, together with cases such as the cutting of cables in Vietnam in 2007 to steal components using rudimentary tools, show that shallow and heavily trafficked maritime environments are inherently exposed spaces. They also demonstrate that large-scale global disruption can be triggered through relatively low-cost interventions.

Building on this awareness of structural vulnerabilities, contemporary military doctrines have incorporated targeted physical sabotage of subsea infrastructure into the operational logic of grey-zone tactics and hybrid warfare. This approach seeks to inflict systematic economic damage on adversaries while remaining below the legal threshold that would trigger an overt conventional response. It relies fundamentally on plausible deniability to limit direct attribution. Early indications of this approach have been observed in the waters of the Arabian Gulf and the Gulf of Oman since 2019, where commercial vessels were targeted using low-intensity explosive devices designed to minimise traceable evidence and obscure the identity of the responsible actor.

These tactics soon expanded to include subsea data networks and underwater energy infrastructure, as became especially clear in the Baltic Sea through a series of sabotage incidents. These included cable disruptions near Norway's Svalbard archipelago in 2022, damage to critical infrastructure in 2023 linked to the vessel NewNew Polar Bear, and the severing of vital cables in late 2024 involving the ship Yi Peng 3. Taken together, these incidents reflect a growing trend toward the weaponisation of ostensibly civilian activity. This trajectory is reinforced by intelligence assessments that documented 42 cable disruption incidents worldwide between early 2024 and mid-2025, around a quarter of which were linked to suspicious anchor-dragging by vessels with opaque ownership structures. These patterns underline the emergence of a strategy in which seemingly routine maritime incidents are repurposed into effective tools of asymmetric conflict.

This pattern of sabotage has since developed into an operational reality within the critical maritime corridors of the Middle East, taking on far greater significance as active military operations increasingly intersect with the security of digital infrastructure. A major turning point came in February 2024, when the incident involving the commercial vessel MV Rubymar in the Red Sea resulted in its uncontrolled drift, severing three major international cable systems.

This incident disrupted nearly 70% of data traffic between Europe and Asia and triggered a complex repair process that lasted six months under conditions of elevated security risk. It was followed by a parallel escalation in September 2025, when multiple disruptions affected critical systems near the western coast of Saudi Arabia. These outages sharply increased latency for cloud service providers and severely disrupted connectivity across major states, including India, Pakistan, and the United Arab Emirates.

These operational realities confirm that contemporary threats can transform congested maritime corridors into zones of comprehensive digital constraint. In such an environment, the threat of cable disruption becomes a tool of deterrence and geopolitical coercion. This dynamic heightens the risks associated with routine maintenance operations and makes the deployment of new network infrastructure far more difficult under volatile security conditions.

The historical evolution of maritime warfare tactics, and their systematic shift toward targeting subsea infrastructure, provides a critical framework for understanding the deeper transformation in contemporary Iranian military doctrine. With the outbreak of confrontation in early 2026 and the resulting constraints on Iran's conventional naval ability to control surface energy transport routes, decision-makers in Tehran appear to have absorbed the strategic lessons drawn from recent operational precedents and grey-zone tactics. At the heart of this recalibration lies a clear recognition of the scale of global disruption that can be generated by exploiting the physical vulnerability of communications networks, combined with a structured reliance on plausible deniability.

This strategic recalibration has taken the form of a sharp tactical shift, reflected in explicit threats to target submarine internet cables passing through the Strait of Hormuz and the Arabian Gulf. Their deliberate disruption is now framed as an asymmetric pressure tool aimed at offsetting power imbalances and destabilising the global digital economy. Yet the transition of these geopolitical threats from strategic signalling to an operational reality capable of producing sustained structural paralysis depends on more than political intent and target value. It also requires a careful assessment of the offensive capabilities of the Islamic Revolutionary Guard Corps Navy, including its technical assets, subsea platforms, and specialised logistical capacities needed to carry out complex physical sabotage operations beneath the seabed and to translate theoretical threats into real operational effects.

III. Assessing the Offensive Capabilities of the Islamic Revolutionary Guard Corps Navy

Strategic assessments broadly agree that the submarine cable infrastructure spanning the Strait of Hormuz faces a complex spectrum of sabotage threats, many of which align directly with the operational capabilities of the Islamic Revolutionary Guard Corps Navy following the degradation of much of Iran's conventional naval forces in recent operations. In this context, Iranian military doctrine has increasingly focused on developing operational systems tailored to the hydrographic conditions of shallow waters and the highly complex acoustic environment of the Arabian Gulf. This adaptation gives Tehran a distinct asymmetric advantage in conducting targeted disruption operations.

These threats can be grouped into three principal operational vectors. The first involves direct human intervention through combat diver units, which offer the highest degree of plausible deniability because deliberate sabotage can be difficult to distinguish from accidental damage caused by maritime anchoring activity. The second centres on the deployment of unmanned underwater vehicles and subsea munitions capable of extended loitering before launching surprise strikes. The third relies on small tactical submarines to deploy intelligent naval mines, a method designed to inflict indirect damage on digital infrastructure by targeting commercial vessels transiting above cable routes and causing them to sink.

Diver Operations

The Islamic Revolutionary Guard Corps Navy Special Force, based on Farur Island, represents the most specialised operational arm for conducting precise sabotage activities in the subsea environment. This elite unit possesses advanced field capabilities, including combat diving, underwater explosive emplacement and disposal, special reconnaissance, and amphibious assault, boarding, and maritime interdiction operations. These capabilities were clearly demonstrated during the seizure of the commercial vessel MSC Aries in April 2024.

These assessments are reinforced by US intelligence evaluations pointing to the existence of a specialised maritime operations unit regarded as the most likely executor of any attack targeting the seabed, drawing on intensive training in the use of magnetic mines and limpet charges. Yet the methods of attack are not limited to the conventional use of high explosives. They also extend to more sophisticated forms of mechanical intervention. Modern fibre-optic cables are protected by dense engineering armour comprising galvanised steel wires and insulating materials, particularly in shallow coastal zones. Breaching them, therefore, requires specialised industrial-grade equipment. In practice, this can be achieved effectively through hydraulic cutting tools, allowing for precise disruption without resorting to explosive methods that would attract immediate attention.

To strengthen these capabilities, Iran has increasingly relied on integrating commercially available technologies into its military systems, bypassing export restrictions through complex intermediary networks operating in jurisdictions such as Georgia and Hong Kong. This approach enables the acquisition of advanced remotely operated vehicles and subsea engineering equipment that require relatively limited operational support and can be deployed covertly via civilian fishing vessels or fast maritime craft.

Once in position, these systems can use high-resolution sonar and imaging technologies to locate buried cables. This provides a cost-effective and highly precise means of disruption while preserving a high degree of operational ambiguity and plausible deniability. The most notable of these systems include:

Ghadir-Class Tactical Mini-Submarines

Alongside human operatives and unmanned systems, the naval structure of the Islamic Revolutionary Guard Corps also relies on Ghadir-class tactical mini-submarines as critical launch platforms for unconventional operations marked by low physical and thermal signatures.

The operational profile of these submarines, designed to function effectively at depths of around 60 metres, aligns closely with the topographical distribution of submarine internet cables across the seabed of the Arabian Gulf and the Strait of Hormuz. Although Iran received an advanced generation comprising dozens of these platforms in 2021, recent intelligence assessments indicate that a substantial portion of this fleet sustained extensive structural damage and a major loss of operational capacity during the direct military confrontations that began on 10 March 2026.

Even so, the remaining or serviceable units continue to pose a serious tactical threat. Operating under the cover of darkness, they can be used to lay naval mines covertly and avoid direct detection. This capability poses a latent threat that could undermine surface maritime security and trigger cascading damage to the digital infrastructure embedded along critical subsea corridors.

Unmanned Underwater Vehicles and Loitering Munitions

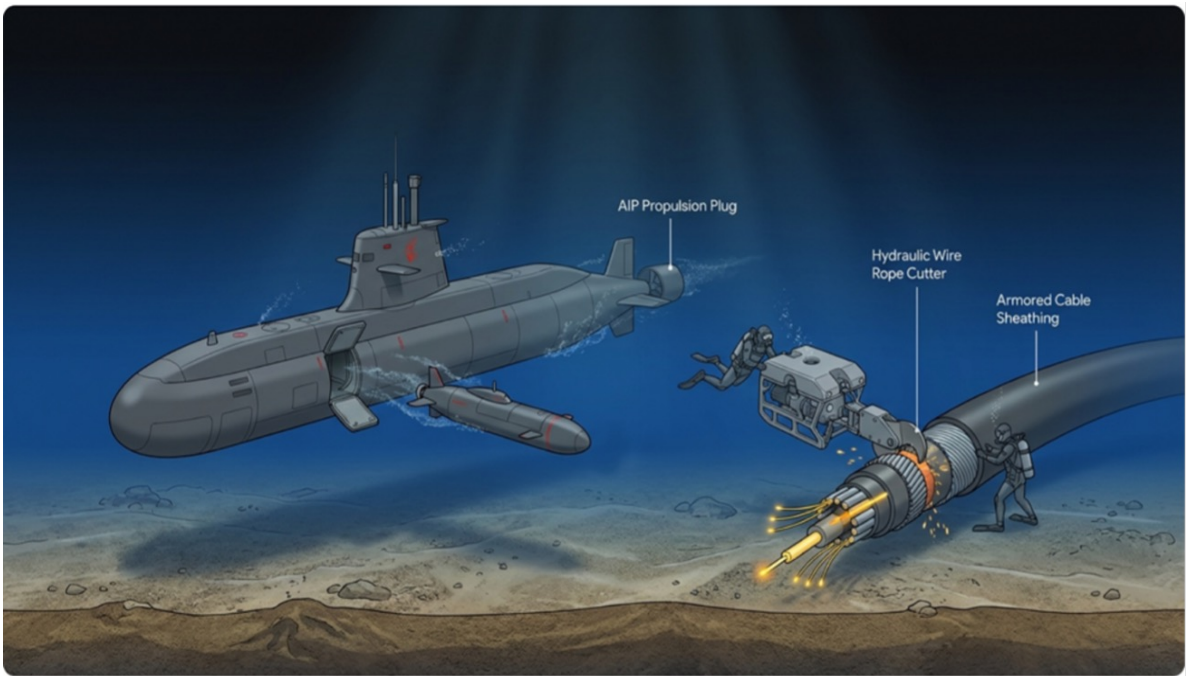
The technological trajectory of Iran's naval arsenal reflects a deliberate and accelerating shift toward deploying autonomous and unmanned subsea systems designed to exploit the geographic constraints of the regional operating environment. At the forefront of these capabilities are platforms such as the Nazir-5 class, which combine torpedo-like hydrodynamic design with autonomous navigation technologies in order to minimise drag and extend operational endurance. These systems can remain deployed for up to 24 hours and operate at depths of up to 200 metres.

They rely on inertial navigation systems to approach pre-designated stationary targets, such as submarine cables and offshore energy infrastructure, at low speeds, enabling them to function as delayed-action strike platforms. Equipped with high-explosive payloads and advanced battery systems, these vehicles can remain dormant without emitting detectable acoustic signatures, increasing their value as covert offensive assets.

This engineering effort is further reinforced by the development of the Azhdar system, an unmanned underwater vehicle derived from torpedo programmes and capable of loitering tactically for up to 96 hours while carrying an explosive payload of around 200 kilograms. This configuration gives it significant strike potential against critical infrastructure targets.

Alongside these offensive systems, analysis of open-source intelligence data and satellite imagery of military facilities in Bandar Abbas since mid-2023 has also revealed the presence of large, high-displacement unmanned underwater vehicles. These advanced platforms are characterised by large internal payload compartments, allowing them to be fitted with robotic manipulators for precise engineering interventions along cable routes or to carry sophisticated intelligence systems for surveillance and reconnaissance. They also show emerging capabilities to deploy offensive drones directly from beneath the surface, further increasing the complexity and multi-layered nature of threats directed at the digital ecosystem.

Figure (3): Simulation of Targeting Mechanisms for Critical Infrastructure



The Expansion of Naval Capabilities Among Regional Armed Factions

The scope of threats facing subsea infrastructure extends beyond Iran's immediate geography and expands structurally through a network of regional armed factions that benefit from the transfer of technology and military expertise in support of overlapping geopolitical agendas. In this context, the Houthi movement in Yemen emerges as a critical operational actor, leveraging its strategic position overlooking the Bab el-Mandeb Strait. This dynamic became clear when US Central Command thwarted an attempted launch of an unmanned underwater vehicle from Yemeni shores in February 2024.

This operational pattern escalated further with the attack on the commercial vessel MV Rubymar, which led to its sinking and caused its anchor to sever three vital international submarine communication systems. The incident disrupted nearly a quarter of total data traffic flowing between Asia, Europe, and the Middle East, providing clear empirical evidence of the deep security vulnerability of this maritime corridor.

These asymmetric capabilities are not confined to the Red Sea theatre but extend to other factions seeking to expand their maritime reach. In the Gaza Strip, early attempts were recorded as far back as 2021 to target offshore gas platforms using unmanned systems, while subsequent assessments indicated the existence of a manufacturing base capable of producing torpedo-like devices with geospatial guidance capabilities.

In parallel, strategic assessments indicate that Hezbollah in Lebanon possesses an advanced arsenal of anti-ship missiles and specialised naval units, as well as the potential to possess modified variants of mini-submarines and unmanned attack platforms. This structured distribution of sabotage capabilities creates a highly dangerous operational environment, raising the possibility of coordinated and simultaneous strategic attacks against the critical infrastructure underpinning the global economy across interconnected theatres, including the Arabian Gulf, the Red Sea, and the eastern Mediterranean.

IV. Iranian Motivations for Targeting Digital Infrastructure

A range of interlinked drivers increases the likelihood that Iran may resort to subsea sabotage as a decisive tool of deterrence or escalation in order to recalibrate the balance of power. These drivers are closely tied to ongoing military, economic, and domestic pressures, and can be grouped into several principal pathways that reflect the scale of existential threats perceived by the regime, as outlined below:

US Ground Insertion and Territorial Incursion into Iran

A potential Iranian shift toward targeting digital infrastructure in the Arabian Gulf is closely tied to the emergence of US military plans involving amphibious and airborne operations to secure a chain of strategically significant islands that would exert control over the maritime domain.

Kharg Island has emerged as the central strategic objective. Located roughly 15 nautical miles off the Iranian coast, it accounts for around 90% of Iran's oil exports, estimated at between 1.3 and 1.6 million barrels per day. The island also holds a strategic reserve of approximately 18 million barrels. On 14 March 2026, its military installations were struck in a precision operation that reportedly destroyed 90 targets without damaging the oil infrastructure. This aligns with reporting by the Financial Times and Axios, which indicate that US policymakers view the island as a critical pressure point to compel Tehran into compliance.

Operational scenarios under consideration include an amphibious landing using medium craft launched from the USS Tripoli, supported by armoured units and HIMARS rocket systems, or an airborne insertion via V-22 Osprey aircraft deployed from the USS Boxer.

In parallel, Qeshm Island, the largest island in the Arabian Gulf at approximately 1,445 square kilometres, presents a highly complex amphibious challenge. Its shallow surrounding waters, close proximity to Iranian coastal artillery, direct linkage to the mainland, and the presence of an extensive tunnel network used to store missiles, unmanned systems, and naval mines collectively make it, according to military assessments, one of the most difficult amphibious objectives to secure.

The targeting matrix also extends to critical chokepoints, most notably Larak Island, located at the narrowest point of the Strait of Hormuz. The island hosts a strategic surveillance and command system supported by a network of hardened bunkers and fast attack craft bases. Securing Larak would deprive Iranian forces of their ability to monitor commercial shipping and disrupt mine-laying operations. This has led US military planners to designate it as an initial operational objective, given its favourable maritime depth outside the confined waters of the Gulf.

The strategic picture is further complicated by the inclusion of the occupied Emirati islands in the conflict calculus, most notably Abu Musa, which carries exceptional diplomatic sensitivity due to its occupation since 1971 and the formal sovereignty claims maintained by Abu Dhabi. Tehran uses the island as a forward base for monitoring and targeting maritime traffic, supporting fast attack craft operations and mine-laying activity within what is described as Iran's defensive arc, a concept viewed by Iranian military leadership as a set of unsinkable aircraft carriers. On March 25, 2026, Iranian Parliament Speaker Mohammad Bagher Ghalibaf stated that Tehran possessed intelligence indicating that regionally backed military preparations were underway to seize one of these islands.

The logistical significance of the other islands varies. Lesser Tunb, an uninhabited island of roughly one square mile inhabited by venomous snakes, represents a relatively accessible military objective but one of limited strategic value. By contrast, Kish Island functions as an economic and maritime support hub, hosting fast-attack craft, although it holds lower military priority due to its relative distance from the main shipping lanes of the Strait.

To achieve these strategic objectives, the United States is assembling a layered strike force comprising several thousand Marines. The USS Tripoli is deploying the 31st Marine Expeditionary Unit, comprising approximately 2,500 personnel, while the USS Boxer is sailing from California with the 11th Marine Expeditionary Unit on a voyage expected to take several weeks. This deployment is being reinforced by elements of the 82nd Airborne Division, bringing the total force allocated for island operations to an estimated 5,000 to 7,000 personnel.

Despite this substantial mobilisation, military assessments indicate that the harsh terrain of these islands, characterised by natural caves, steep escarpments, narrow shorelines, and limited escape routes, would make any amphibious landing a highly complex operational undertaking. Crucially, such operations would not necessarily eliminate Iran's residual ability to threaten the Strait.

In this operational context, Iranian leadership is likely to view any infringement on its sovereignty over these positions, particularly Kharg Island, as a direct threat to the structural foundations of its national economy and its core revenue streams. Faced with the limits of conventional military options to alter the balance of power against the coalition, Tehran would likely be pushed toward an asymmetric response strategy, making the targeting of submarine cable networks a principal operational option to shift the confrontation onto the global stage and impose parallel disruption on the international economy.

Targeting Infrastructure and Energy Facilities

The trajectory of asymmetric escalation through sabotage would be significantly reinforced if coalition operations were expanded to include concentrated strikes against power generation facilities and critical infrastructure within Iranian territory. This escalation pathway became evident following the announcement by President Trump on March 26, 2026, via Truth Social, of a temporary 10-day suspension of planned strikes on Iranian energy facilities, until 6 April. The delay was presented as a response to the Iranian government's request to allow time for negotiations.

This announcement made clear that the strategic target set remains immediately actionable should the diplomatic track collapse, signalling readiness to strike the country's largest power-generation facilities. Iran's national energy system depends overwhelmingly on more than 130 gas-fired thermal power plants, which together generate over 75% of the country's electricity demand, with a total deliverable capacity of approximately 62,000 megawatts. This network includes around twenty plants with capacities exceeding 1,000 megawatts each, while three major facilities surpass the 2,000-megawatt threshold.

The most acute strategic vulnerability is concentrated in the geographic belt surrounding Tehran, which forms the core of the state's operational and administrative system. Five major power plants, Damavand, Rajaei, Montazer Ghaem, Rudshur, and Mofatteh, collectively make up the capital's critical electricity supply network. A coordinated strike against this cluster would likely trigger a comprehensive power outage across a metropolitan area of approximately 16 million people, paralysing government and military command-and-control structures.

The threat is not confined to conventional infrastructure. Still, it extends to highly sensitive facilities, most notably the Bushehr nuclear power plant on the Gulf coast, Iran's only nuclear energy facility, with a capacity of approximately 1,000 megawatts. The Director General of the International Atomic Energy Agency, Rafael Grossi, has issued explicit warnings that any strike on this facility would represent a dangerous breach of nuclear safety thresholds and could trigger a severe environmental disaster through widespread radioactive contamination of Gulf waters.

The destruction of such critical assets would trigger a sharp collapse in national energy supply and prolonged outages, inevitably degrading the efficiency of logistical supply chains and internal communications networks on which military institutions depend. Under such acute structural pressure, Iranian leadership would likely seek to externalise the crisis by using maritime infrastructure as a strategic instrument, grounded in the logic of reciprocal strategic harm. In practice, the disabling of domestic energy networks and the isolation of command centres would be met with systematic efforts to induce digital disruption and paralysis across international financial systems, thereby imposing economic costs on a scale that could exceed the international community's capacity to contain.

Support for Separatist and Ethnic Movements

Direct military pressure intersects with internal stability dynamics to form a central determinant of Iran's strategic response pathways, particularly given the country's complex demographic composition, in which ethnic Persians account for only around 51% of the total population. Major ethnic minorities are concentrated along the geographic periphery, forming, strategically, a secession-prone territorial belt. This constitutes a structural security vulnerability that hostile military strategies, led by the United States and Israel, may seek to exploit by activating internal fronts and providing logistical and military support alongside direct strikes.

The most significant pressure point lies in the western provinces, including Kurdistan, Kermanshah, and West Azerbaijan, where the Kurdish population accounts for approximately 10 to 12% of the total, estimated at around 12 million people. In this theatre, six armed factions based in Iraqi Kurdistan had aligned prior to the outbreak of the conflict. Foremost among them is the Kurdistan Democratic Party of Iran, the oldest and largest of these groups, whose leader, Hafiz Hussein, is reported to have held direct telephone contact with US officials. This alignment also includes the Komala Party, with its pluralist socialist orientation, and the Kurdistan Free Life Party, the Iranian branch of the Kurdistan Workers' Party, alongside the Khabat Organisation and two additional factions with active military wings.

This pattern of internal attrition also extends to the south-eastern front in Sistan and Baluchestan province, bordering Pakistan and Afghanistan, where Baluchi militancy intensified following the merger of Jaish al-Adl with smaller local factions to form the Popular Resistance Front in late 2025. This group derives much of its operational significance from substantial field experience, demonstrated in an attack on security forces in April 2024 that killed 21 personnel. Its capabilities are further reinforced by partial access to US-origin equipment smuggled from Afghanistan.

Within the same geostrategic framework, Khuzestan province, which holds approximately 80% of Iran's oil reserves, represents the principal strategic prize for adversarial planning. Armed Arab Ahwazi factions operate in this region, including the Arab Struggle Movement for the Liberation of Ahvaz and the Arab Region Organisation. In March 2026, Iranian security authorities announced the dismantling of an armed cell within the province, alleging that it had received financial support from US and Israeli sources.

The strategic picture is further complicated by the Azerbaijani minority, which constitutes the largest ethnic bloc and is estimated at between 15 and 20 million people. Reports suggest that Washington and Tel Aviv have exerted sustained pressure on Azerbaijani President Ilham Aliyev to align with the opposing axis, accompanied by geopolitical assurances tied to ambitions for a "Greater Azerbaijan" through the incorporation of Iran's north-western regions. While the Pentagon has included the Mujahedin-e Khalq within its broader alignment as a political entity in exile, its limited domestic support and widespread scepticism among analysts regarding its effectiveness as an instrument of change have meant that reliance remains centred primarily on ethnically based movements.

Faced with this existential threat to the cohesion of its central state institutions, Tehran would likely resort to signalling the potential disruption of submarine cable networks in order to trigger a global financial and technological shock. Such a move would aim to compel neutral actors to intervene urgently and to impose a negotiating framework in which the coalition would be required to halt its support for separatist movements as a precondition for restoring stability to the global digital economy.

Tactical Nuclear Targeting

At the highest threshold of escalation, far beyond the signalling of geopolitical pressure, lies the possibility that the United States could resort to low-yield tactical nuclear munitions to penetrate and destroy heavily fortified Iranian military facilities embedded in mountainous terrain. In parallel, the potential activation of Israel's doctrine of comprehensive deterrence, commonly referred to as the Samson Option, represents an additional vector of extreme escalation.

This development, with its immense destructive potential and its decisive breach of internationally recognised red lines, would amount to a complete collapse of conventional deterrence frameworks and a fundamental abandonment of strategic proportionality. Faced with a level of targeting that would be perceived as existential, the Iranian military establishment would likely abandon any remaining constraints tied to restraint or calibrated diplomatic calculation. Such an action would be interpreted as definitive confirmation of the state's long-standing narrative that external actors seek to eliminate the regime, thereby driving the adoption of a comprehensive offensive strategy unconstrained by conventional political limits.

Under such an extreme escalation scenario, the role of maritime infrastructure would undergo a profound doctrinal shift. The targeting of fibre-optic networks across the seabed of the Arabian Gulf and the Red Sea would move from a limited tactical tool of negotiation and deterrence to a central instrument of comprehensive strategic retaliation.

At this stage, the objective would extend beyond temporary disruption of communication flows. It would become a sustained effort to impose structural and potentially irreversible paralysis on digital systems and financial clearing networks that underpin the global economy, as a reciprocal response to the non-conventional damage inflicted on Iranian territory. Assessments further suggest that such a digital offensive would be accompanied by a large-scale campaign involving the dense and indiscriminate deployment of intelligent naval mines across critical maritime corridors.

This dual approach would aim to enforce both physical and digital blockades, generating a prolonged global economic and logistical shock. Under these conditions, systemic breakdowns would emerge as a direct consequence of a regional conflict escalating into the actual use of nuclear weapons.

V. Affected Stakeholders

The foundational architecture of the global internet is built on dynamic data-routing protocols, most notably the Border Gateway Protocol, which serves as a core software mechanism designed to preserve continuity by automatically rerouting traffic through alternative pathways whenever disruption is detected at a given node or along a route. Yet the operational effectiveness of this advanced technical mechanism is constrained by a major physical and structural limitation when applied to maritime corridors in the Middle East. The sheer volume and density of intercontinental data traffic passing through this region exceed the capacity of any available alternatives, sharply limiting the system's practical resilience.

In a scenario involving large-scale sabotage of subsea cable systems, both maritime backup routes and terrestrial fibre alternatives would be immediately saturated. This abrupt and forced redirection of data traffic would cause severe network congestion, leading to substantial packet loss and a sharp rise in latency to levels that disrupt core operations. Under such conditions, structural outages in communication services would become increasingly likely, isolating vast geographic areas and triggering deep economic and logistical repercussions.

The coastal states bordering the Arabian Gulf would stand on the front line of any large-scale disruption to data flows, with their economic and digital systems bearing the brunt of the resulting structural paralysis. The severity and depth of these effects would vary from one country to another, shaped by a set of strategic variables, including the resilience of alternative infrastructure, the carrying capacity of terrestrial transmission routes, and the geographic positioning of submarine cable landing stations that link domestic networks to the global internet backbone.

The United Arab Emirates and the Sultanate of Oman

The United Arab Emirates and the Sultanate of Oman serve as the principal hubs for managing and transiting digital data flows across the region, yet both face security exposures closely tied to their infrastructure configurations. The UAE benefits from a major geostrategic advantage by concentrating many of its critical international cable landings in Fujairah, located on the Gulf of Oman, outside the constrained, high-risk confines of the Strait of Hormuz. This positioning provides a comparatively secure routing option, allowing a substantial share of regional data traffic to bypass the most volatile maritime corridor.

In parallel, Oman has pursued an expansive strategy to strengthen its position in the digital data centre sector. It currently hosts 21 submarine cable systems, including planned and under-construction projects, with a strategic concentration of landing stations in Muscat and Salalah. To improve operational resilience and secure reciprocal routing capacity, the two countries have recently activated the Oman–UAE Gateway, a 275-kilometre advanced subsea cable system designed to connect critical data hubs, linking the Equinix MC1 facility in Oman with the Datamena DX1 centre in Dubai.

Despite these substantial infrastructure investments, the technology sector remains exposed to acute systemic risk. The UAE's major investments in artificial intelligence infrastructure, including a $15.2 billion joint initiative between Microsoft and G42, as well as ambitious plans to develop hyperscale computing facilities with a projected capacity of 5 gigawatts, remain directly vulnerable to geopolitical disruption.

Recent operational targeting of Amazon Web Services facilities through drone attacks has shown that advanced physical and digital infrastructure in the Gulf is directly exposed to the spillover effects of regional conflict. This dynamic raises the risk of disruption or suspension of multi-billion-dollar investments in the artificial intelligence sector if connectivity to the global network becomes insufficient or unstable.

The Kingdom of Saudi Arabia

Saudi Arabia's digital strategy is anchored in geographic diversification that provides a degree of structural protection. The majority of its international bandwidth is routed through primary landing stations along its western Red Sea coastline, particularly in Jeddah, giving the country significant resilience against potential large-scale disruptions in Gulf waters. However, this relative insulation does not extend to the Eastern Province, which is the core of the national economy, serving as the main hub for oil extraction, refining, and energy exports. This critical region remains heavily dependent on communication channels routed through the Arabian Gulf.

In the event of sabotage affecting submarine cables, the complex industrial operations of this sector would face serious disruption to the digital command-and-control systems on which facility operations depend. These risks are further amplified by Saudi Arabia's strategic push to localise artificial intelligence capabilities and cloud computing infrastructure. This direction is reflected in major initiatives, including the development of an integrated cloud region by Amazon Web Services valued at $5.3 billion, and the establishment of an advanced artificial intelligence centre in partnership with Google near Dammam, with investments estimated at $10 billion. Systematic disruption of subsea transmission routes in Gulf waters would create severe data-flow bottlenecks and processing constraints affecting data centres in the Eastern Province. This, in turn, would inevitably degrade the operational efficiency of the critical energy sector and undermine the foundations of the Kingdom's emerging digital economy.

Kuwait, Bahrain, and Qatar

Kuwait, Bahrain, and Qatar face a highly constrained and vulnerable strategic position, shaped by their geographic confinement within the Arabian Gulf's enclosed basin. Although these states maintain limited terrestrial connectivity options, including links to Saudi Arabia and, in Kuwait's case, extensions toward Iraq, a simultaneous and comprehensive disruption of submarine cable systems would quickly overwhelm these land-based routes. Structurally, such alternatives lack the multi-terabit transmission capacity of modern subsea systems, rendering them unable to absorb the full volume of redirected data traffic.

This would cause severe congestion in data flows, sharply deteriorating internet speeds and triggering immediate economic and commercial contraction across all critical sectors. The scale of these repercussions is especially evident in Qatar, where digital paralysis would threaten the highly complex logistics systems that manage and support large-scale liquefied natural gas extraction and export operations in Ras Laffan Industrial City, thereby disrupting energy supply stability.

In Bahrain, which has established itself as a key regional financial and banking hub, such disruption would pose a direct threat to financial-sector operations, already under pressure from advanced cyber threats and physical security risks. This vulnerability was clearly exposed by the damage sustained by Amazon Web Services data centres within its territory following recent drone attacks, further amplifying the scale of financial and digital exposure.

Iraq and Iran

Iraq is pursuing a determined strategy to reduce its historical dependence on oil revenues by investing in its role as a key digital land bridge linking Asia and Europe. This approach is intended to provide a secure alternative route that bypasses recurring bottlenecks in congested Red Sea corridors. It is being advanced through government-led projects to expand landing and reception stations at the Al-Faw Grand Port in Basra, with the aim of integrating Iraqi territory into major international communication systems, including the planned 45,000-kilometre 2Africa cable, alongside participation in the Gulf's regional fibre-optic network.

However, any large-scale disruption to submarine cables in Gulf waters would immediately paralyse this emerging digital transit economy on which Iraq relies to diversify its revenue base, thereby undermining its broader geoeconomic ambitions.

Figure (4): Cost of a 24-Hour Internet Disruption

Country	Internet Users	Est. 24-Hour Outage Cost	Recorded Annual Shutdown Losses
India	755,820,000	$920 Million	$179 Million (2025)
United Arab Emirates	8,913,217	$460 Million	N/A
Saudi Arabia	N/A	N/A	$465 Million (2016)
Iran	71,940,000	$37.4 Million	$214.7 Million (2025)
Iraq	39,600,000	N/A	$595 Million (2025)
Pakistan	82,900,000	N/A	$1.13 Billion (2025)
Austria	7,681,957	£372.2 Million	N/A
Italy	36,387,619	£344.0 Million	N/A
Denmark	5,407,278	£320.5 Million	N/A

Table: Al Habtoor Research Centre • Created with Datawrapper

Conversely, Iran would face acute digital isolation, undermining the integrity of its internal data infrastructure, intensifying the effects of existing international economic sanctions, and deepening its structural vulnerabilities. Even so, Iran's understanding of asymmetric warfare drives both Tehran and its regional proxies to exploit the Strait of Hormuz's fragility as a highly consequential geopolitical lever. By placing a vast share of global internet traffic passing through these digital corridors at risk of disruption, these actors could exert disproportionate strategic influence and inflict substantial structural economic damage on Gulf Cooperation Council states and the wider global financial system, achieving long-term objectives without engaging directly in costly conventional warfare.

Cascading Network Effects on Global Nodes

This abrupt and forced redirection of data traffic would generate severe network congestion, manifested in substantial packet loss and a sharp rise in latency to levels that disrupt operational processes and ultimately produce structural outages capable of isolating vast geographic areas. Accordingly, the systematic disruption of cables in the Strait of Hormuz and the Arabian Sea would not be confined to regional effects. It would instead trigger immediate cascading failures across dependent economies located thousands of miles away, transforming a geographically contained geopolitical conflict into a global economic and technological crisis that strikes at the core functions of the international system.

India and South Asia

The Indian subcontinent, and South Asia more broadly, exhibit an exceptional degree of structural vulnerability to disruptions in digital infrastructure across the Arabian Gulf and the Arabian Sea, owing to their near-total reliance on westward-oriented submarine cable networks. This dependency is reflected in the heavy reliance on critical systems, most notably the SEA-ME-WE (Southeast Asia-Middle East-Western Europe) cable consortium across its third, fourth, and forthcoming sixth generations, alongside systems such as FALCON, the India–Middle East–Europe Gateway, and the Tata Global Network Gulf.

This critical connectivity forms the backbone of India's information technology and business process outsourcing sector, with an estimated market value of around $270 billion, whose operational continuity depends on sustained high-speed links with client bases in Europe and the Middle East. Any physical disruption to these maritime routes would trigger sharp and unprecedented increases in network latency.

This was demonstrated by the Red Sea disruptions in September 2025, which led to latency increases of between 20 and 30% across key nodes linking Mumbai and Delhi with London and Frankfurt. Such immediate technical degradation would result in significant breaches of service-level agreements, substantial losses in overall productivity, and the effective paralysis of high-frequency financial trading systems that depend on ultra-low latency and precise real-time processing.

In addition to institutional impacts, India's domestic networks, which serve approximately 364 million 5G subscribers with the highest global data consumption rate of around 24 gigabytes per user per month, would face a heightened risk of systemic strain due to the sudden shock to international capacity feeding these systems. At the macroeconomic level, such a disruption would introduce significant delays in remittance flows from expatriate workers in Gulf states, which exceed $30 billion annually, thereby amplifying economic repercussions and intensifying financial and social pressures in New Delhi.

East Africa

The systemic impact of disruptions to maritime network infrastructure extends to East African states, most notably Kenya, Djibouti, Tanzania, and Mozambique, whose digital architectures are strategically dependent on cables routed from Asia via the Arabian Sea and the Gulf of Oman, including systems such as PEACE, SEACOM, and the East African Submarine Cable System, which underpin their connectivity to the global internet backbone. The region's emerging digital economy constitutes a key engine of growth, with millions of small and medium-sized enterprises relying daily on the stability of digital tools, mobile financial services, and logistics platforms that support cross-border trade.

Any physical disruption to these critical corridors would immediately paralyse electronic financial transaction pathways and the export of digital services. The region has already experienced the practical implications of such scenarios during the outages affecting SEACOM and the East African Submarine Cable System in May 2024, which exposed the rapid vulnerability of countries such as Tanzania and Mozambique to sudden and severe connectivity failures. Moreover, high-capacity infrastructure projects such as the PEACE cable contribute directly to the gross domestic product of host countries with landing stations, including Djibouti and Kenya, generating millions of dollars in economic value.

The loss of this core connectivity would extend far beyond short-term revenue losses. It would also undermine institutional confidence in business stability, discourage foreign direct investment into the financial technology sector, deepen the digital divide, and constrain pathways to inclusive development across the African continent.

Europe and Southeast Asia

Physical sabotage of submarine cables in the Middle East would directly disrupt the strategic digital corridor linking major data processing hubs in Europe with their counterparts in Southeast Asia. More than 90% of total communications and data exchange between the two regions relies on this maritime route as the most efficient transmission artery.

The severity of such disruption is particularly evident in Asia, as exemplified by Singapore, which serves as the central node for managing regional digital operations. More than 99% of its international communications traffic is routed through submarine cable systems. A digital outage in Middle Eastern waters would therefore interrupt the real-time flow of highly sensitive financial data between major centres such as London and Singapore, leading to temporary systemic failures that could disrupt the continuity of central clearing houses and international payment service providers.

On the European side, strategic significance is concentrated in critical landing stations along the Mediterranean, most notably Marseille, which alone hosts 15 international cable systems, as well as key infrastructure in Sicily. These locations serve as principal gateways for receiving and distributing data flows originating from Asia and Africa into the European core, making them central to the continent's digital connectivity architecture.

When critical transmission systems such as the Asia–Africa–Europe-1 cable and the SEA-ME-WE consortium suffer simultaneous disruption within the Middle East theatre, European hubs would experience an immediate and significant decline in inbound data volumes. This abrupt contraction would compel major global cloud service providers, including Microsoft Azure and Google Cloud, to activate emergency protocols and implement forced traffic rerouting.

These alternatives would typically involve redirecting data through longer Pacific routes or through constrained terrestrial networks, both of which would produce substantial performance degradation. Such emergency measures would inevitably lead to higher packet-loss rates and impose unprecedented structural strain on the global internet's overall capacity, thereby undermining its stability and operational integrity.

VI. Implications of Targeting Submarine Cables

Reducing the function of high-speed internet networks to civilian communication and entertainment media reflects a strategically flawed assessment that overlooks the structural complexity of the modern state. In operational terms, submarine fibre-optic networks form the physical foundation and backbone on which critical national infrastructure and contemporary military operations depend, while also serving as the lifeblood of global strategic commodity markets.

The importance of this connectivity extends well beyond meeting individuals' daily needs. It constitutes a fundamental requirement for the continuity of state institutions and industrial systems. Accordingly, any sustained disruption to data flows across maritime corridors in the Middle East would inevitably produce systemic paralysis across the core nodes of critical sectors, transforming a temporary digital disturbance into a comprehensive functional breakdown that threatens the stability of economic and logistical systems, as outlined below.

Energy Extraction and Logistics

The economic systems of the Gulf Cooperation Council states are structurally dependent on hydrocarbon extraction and refining sectors, which have undergone profound technological transformation and are now fully integrated into advanced digital systems. Modern oil and gas facilities are managed through complex networks of supervisory control and data acquisition systems (SCADA) and industrial control systems that require continuous, high-speed connectivity to central command centres.

This advanced digitalisation is clearly reflected in major facilities such as the Abqaiq complex operated by Saudi Aramco, which processes a critical share of global oil supply. Its dedicated Fourth Industrial Revolution centre relies heavily on real-time data analytics, artificial intelligence applications, and robotic monitoring through unmanned aerial systems to optimise production flows, anticipate maintenance needs, and ensure environmental safety.

In parallel, Abu Dhabi National Oil Company (ADNOC) employs its Panorama Digital Command Centre to aggregate and analyse millions of real-time data points across global supply chains, an initiative that has generated documented commercial returns exceeding $1 billion. These centralised systems and remotely managed operations depend on a continuous, high-volume flow of data from offshore drilling platforms and remote export terminals to sustain production continuity.

Ensuring the continuity of these advanced robotic operations, AI-driven digital twin applications, and high-definition video transmission requires exceptionally high data throughput combined with ultra-low latency. In practical terms, this requirement can only be met through terrestrial and submarine fibre-optic networks, far beyond the capabilities of traditional monitoring systems that relied primarily on geostationary satellite communications.

In the event of large-scale physical disruption to submarine cables, operators of critical facilities would be forced to rely on terrestrial backup routes and on emerging low Earth-orbit satellite networks, such as SpaceX's Starlink and Amazon's Project Kuiper. While these systems can sustain baseline telemetry and emergency communications, they are structurally unable to provide the aggregate bandwidth required to handle the petabyte-scale data volumes needed for hyperscale cloud synchronisation and real-time artificial intelligence operations in major industrial complexes. As a result, severe constraints would be imposed on operational continuity and performance.

The sustained drive to maximise production efficiency, integrate artificial intelligence analytics, and deploy cloud-connected predictive maintenance has led to the near abandonment of the traditional cybersecurity model based on the full physical isolation of operational technology from internet-connected information systems. As a result of this convergence, any physical disruption to submarine cables would immediately sever connectivity between remote sensing units, programmable logic controllers on offshore drilling platforms, remote pipeline nodes, and centralised operational control centres.

In the absence of this critical data flow, automated control systems that enable real-time monitoring and management of pipeline valves, pumping stations, refinery pressures, and export terminals would fail, forcing operators to deploy field teams to manage these systems manually.

In highly complex hydrocarbon environments marked by extreme operational pressures, such slow and manual interventions would sharply increase the risk of catastrophic mechanical failure, toxic leaks, and the forced suspension of production. These risks are reinforced by historical precedents that exposed the sector's technological vulnerabilities, such as the Shamoon malware attack in 2012, which paralysed 30,000 workstations across Saudi Aramco and RasGas.

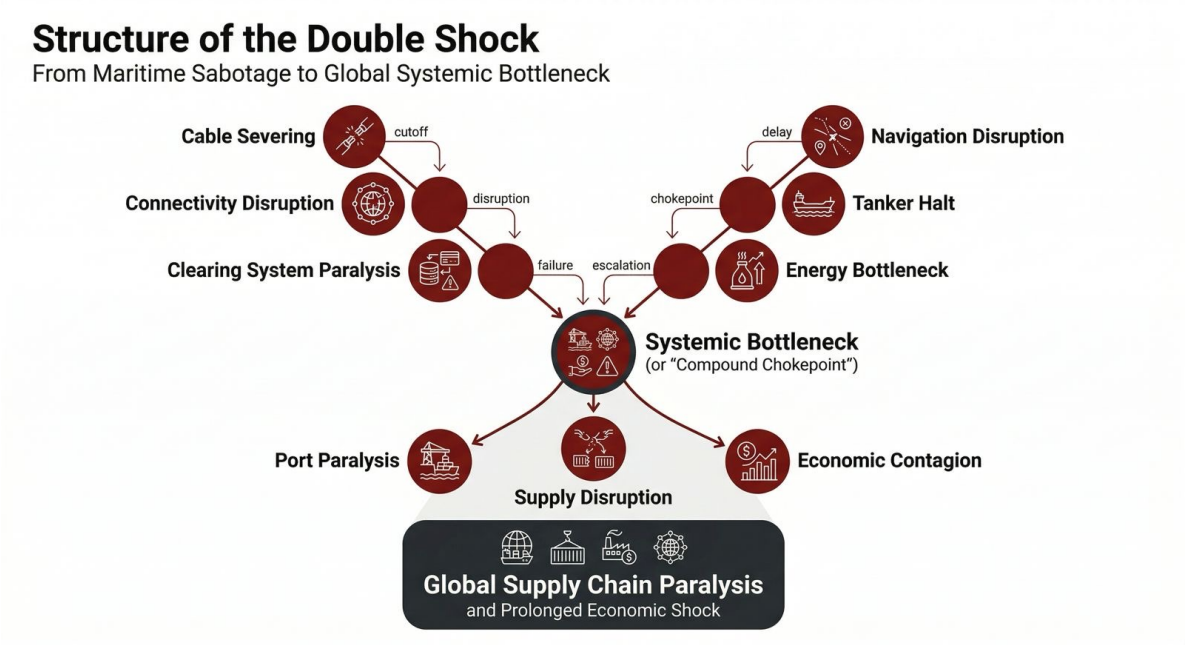
Yet the systemic disruption caused by the physical severance of submarine cables would be considerably more severe, approaching in depth the impact of the 2025 Iberian Peninsula power outage, when failures in SCADA systems left approximately 1.2 million people without electricity for 72 consecutive hours.

Beyond deep operational paralysis, the physical disruption of submarine cables would also create cyber vulnerabilities with highly destructive implications for critical infrastructure. Such disruption would generate widespread disorder and structural instability across technical networks. Under pressure to restore partial connectivity and preserve essential operations, engineering and IT teams would likely be forced to deploy improvised network solutions and bypass established security protocols and technical safeguards.

This transitional phase, marked by operational disorder and weakened controls, would create an ideal strategic window for state-backed actors to launch sustained and sophisticated cyber operations, exploiting emergency conditions to target energy infrastructure and compromise sensitive systems.

Past incidents reinforce this risk, including the deployment of Triton malware, which directly targeted safety instrumented systems at a Saudi petrochemical facility, and the Industroyer 2 attack, which aimed to disrupt energy provider networks in Ukraine. These cases show that breaches during periods of weakened physical infrastructure can lead to severe, potentially irreversible physical consequences. Accordingly, this dual-layered targeting dynamic represents a compounded threat capable of simultaneously destabilising the energy sector at both the digital and operational levels.

Figure (5): The Architecture of Dual Shock Following Submarine Cable Targeting



Economic Implications of Targeting Submarine Cables

The global economy has undergone a rapid acceleration in digital transformation, outpacing the structural resilience provided by the underlying physical infrastructure of submarine communication networks. This imbalance creates a highly precarious condition in which any coordinated targeting of cable routes in the Middle East would act as a direct trigger for a systemic economic crisis with far-reaching regional and global repercussions. The consequences of such disruption would extend well beyond isolated technical failures, constituting a direct threat to the global financial system, which has become fundamentally dependent on high-frequency trading algorithms as a core operational mechanism.

This advanced investment model depends on ultra-low latency, allowing automated systems to exploit instantaneous price differentials across globally distributed exchanges. When direct connectivity routes are physically disrupted, network protocols are forced to reroute dense data flows through longer and heavily congested alternatives, inevitably producing critical delays and increased packet loss. Such technical degradation would severely disrupt algorithmic trading models and generate tangible financial losses for major investment institutions operating across tightly interconnected European, Middle Eastern, and Asian markets.

Regional Sovereign Platforms and Systemic Liquidity Risks

Cross-border payment systems, daily financial settlements, and trading operations managed by sovereign wealth funds would face acute strategic exposure in the event of disruption to digital infrastructure, particularly given established estimates that approximately $10 trillion in global financial transactions flow daily through submarine cables. In an institutional effort to reduce historical dependence on US dollar-denominated correspondent banking networks and strengthen regional financial sovereignty, Gulf Cooperation Council states and the wider Arab region have developed advanced sovereign clearing systems.

In this context, key platforms include the Arab Regional Payments System (Buna), operated by the Arab Monetary Fund, and the Gulf Payments System (AFAQ), both of which provide real-time gross settlement across borders in multiple currencies. These critical platforms rely on stringent messaging standards, particularly ISO 20022, to ensure immediate and accurate transaction validation. Given that such systems depend on continuous, highly secure network synchronisation between regional central banks, participating commercial banks, and global payment networks, including Mastercard Move, which has recently been integrated as a direct participant in Buna, any latency caused by widespread cable disruption would result in an immediate halt in transactions and settlement failure.

A prolonged outage would pose a severe operational and systemic risk, potentially freezing regional liquidity, disrupting foreign exchange pricing mechanisms, and interrupting international remittance flows, which constitute a vital source of income for millions of expatriate workers.

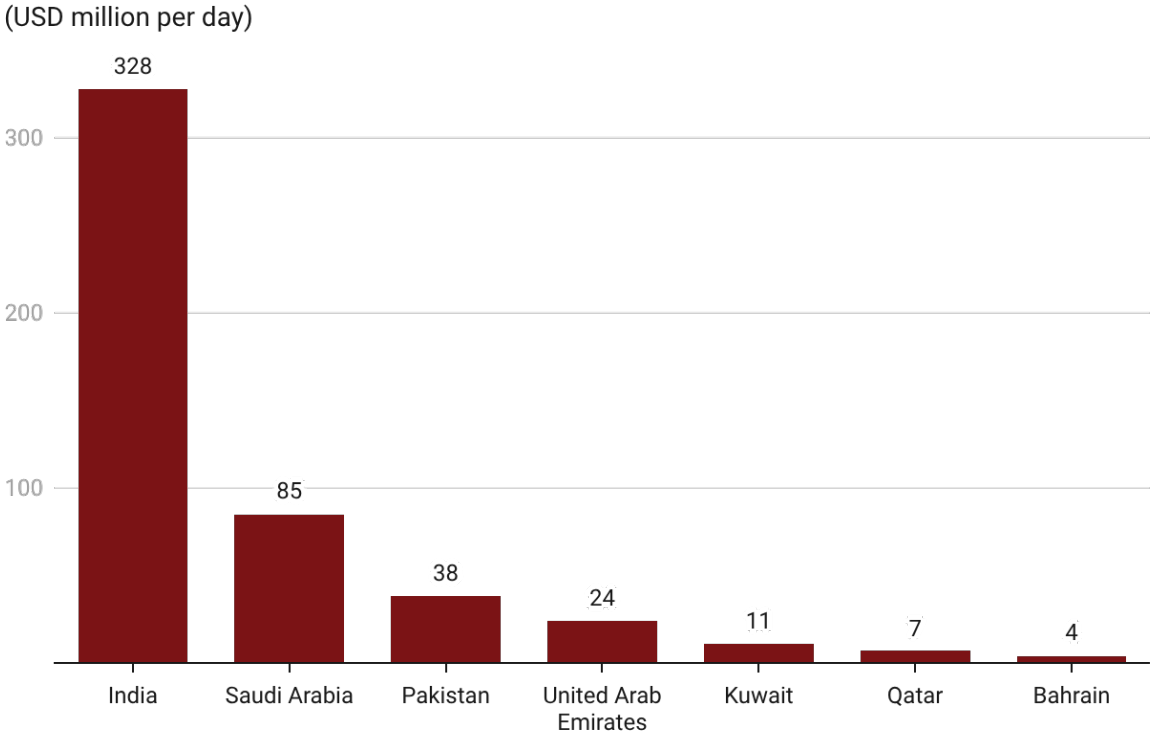
Banking Services, Financial Clearing, and Dependence on the SWIFT System

These implications are further amplified by the central role of the Gulf Cooperation Council states as global financial hubs and critical intermediaries between Eastern and Western financial markets. The regional banking system depends fundamentally on resilient infrastructure to sustain real-time payment flows. Regional settlement platforms, alongside the global financial messaging network SWIFT, require uninterrupted international connectivity to facilitate multi-currency transactions, enforce anti-money laundering protocols, and support real-time gross settlement operations.

Any physical disruption to submarine cable networks would halt data flows across these sensitive financial channels, interrupt trade finance mechanisms, delay institutional settlements, and paralyse the daily operations of major regional stock exchanges.

Regional capital markets, including Saudi Tadawul Group, Abu Dhabi Securities Exchange, and Dubai Financial Market, have recorded significant growth in international participation. This trend is clearly reflected in the expansion of the Qualified Foreign Investor programme, which contributed to a 300% increase in foreign investment in the Saudi market by 2022. A sudden and prolonged disruption to data flows would impose forced isolation on these exchanges, effectively trapping foreign capital and undermining international investor confidence in the resilience and efficiency of the regional financial environment.

Figure (6): Estimated GDP Losses from Internet Disruption



India and Pakistan (partial impact)

Chart: Al Habtoor Research Centre • Source: Deloitte/GNI Framework • Created with Datawrapper

At the broader economic and commercial level, the stability of international financial operations is intrinsically tied to the integrity of digital corridors, particularly the networks that process large-scale daily settlements estimated at approximately $10 trillion. Any simultaneous disruption across geopolitical chokepoints, such as the Strait of Hormuz and the Red Sea, would severely impede cross-border clearing operations, inflict substantial damage on cloud-based supply chain management systems relied upon by multinational corporations, and disrupt decentralised finance platforms and digital asset trading. At the macro-risk level, specialised economic models estimate that a comprehensive internet outage could impose losses of approximately $43 billion per day across the global economy.

Major economies would bear the heaviest share of these losses, with estimated daily costs reaching approximately $11 billion for the United States, $10 billion for China, $3 billion for the United Kingdom, $2.7 billion for Japan, and $1.5 billion for Germany. These quantitative indicators confirm that targeting digital infrastructure in critical maritime corridors would not constitute a confined regional security threat, but rather an asymmetric and far-reaching global economic crisis capable of disrupting the core functions of the international economic system.

Figure (7): Estimated Daily Economic Losses from a Global Internet Outage (USD billions)

Global Total	43
United States	11
China	10
United Kingdom	3
Japan	2.7
Germany	1.5

Logistical Implications of Infrastructure Disruption

The structural effects of disruptions to digital communications infrastructure extend beyond immediate technical failures, exerting profound consequences for economic development trajectories across the Middle East and South Asia. In India, where the economic model remains heavily anchored in the information technology services sector, analytical estimates suggest that potential daily financial losses from such disruption could reach approximately $184.986 million.

These structural effects would extend correspondingly to Gulf Cooperation Council states, particularly the United Arab Emirates, which has adopted advanced strategies centred on digital transformation and artificial intelligence as part of its effort to reduce reliance on hydrocarbon revenues. Any disruption affecting advanced financial operations and cloud data centres would pose a direct challenge to the foundations of these development strategies, thereby weakening the region's competitive positioning as both a regional and global hub for business and investment.

The geopolitical and economic repercussions would not be confined to financial and digital domains, but would extend deeply into the structure of logistical systems and global energy trade, underscoring the intrinsic link between uninterrupted data flows and the efficient management of supply chains. The physical transport of crude oil, refined petrochemicals, and liquefied natural gas is fundamentally dependent on continuous digital connectivity. In this context, the Strait of Hormuz constitutes a critical maritime corridor through which approximately 20% of global liquefied natural gas and around 30% of seaborne oil transit each day. Disruption to submarine cable networks would cause severe disruption to maritime navigation across both the Strait of Hormuz and the Bab el-Mandeb, given the reliance of modern tankers on these networks for navigation tracking and operational coordination.

The severity of this exposure was clearly demonstrated during the 2026 escalation, when deliberate interference with positioning systems and the forced deactivation of tracking devices by vessel crews led to a sharp decline in daily transit rates through the Strait, falling from an average of between 87 tankers to approximately 10. This abrupt contraction in supply triggered an immediate surge in Brent crude prices of more than 42%, prompting countries such as Saudi Arabia to accelerate the diversion of oil exports through alternative routes, most notably the Petroline pipeline to the Red Sea.

The severity of these overlapping crises is further compounded by operational and field constraints that make rapid infrastructure repair exceptionally difficult. The global maritime sector faces a severe shortage of cable repair vessels, with only around 60 in service worldwide. While standard repair operations typically require approximately 40 days per cable under normal conditions, these timelines would likely extend significantly in conflict zones, where civilian operators are reluctant to deploy technical crews. This challenge has already materialised in practice, as specialised firms such as Alcatel Submarine Networks have invoked force majeure, suspending the deployment of repair vessels to avoid operating within active conflict areas.

In parallel with these operational constraints, a structural crisis is emerging within the international marine insurance sector, which serves as the primary financial guarantor for sustaining and underwriting cable projects and maritime operations. As asymmetric threats intensify, particularly given the stark imbalance between the low operational cost of unmanned systems and the high capital value of targeted assets, leading global insurance and reinsurance firms have increasingly invoked war-risk exclusion clauses.

This trend has resulted in the withdrawal of insurance coverage for infrastructure projects and maintenance vessels operating in geopolitically volatile areas of the Middle East, or the imposition of prohibitively high premiums that undermine their economic viability. These financial constraints are further intensified by the potential automatic activation of sensitive exclusion clauses, including those linked to armed conflicts involving the five major powers. Such provisions trigger the immediate and total termination of insurance coverage upon any direct or indirect military involvement by these states within the operational theatre.

Maritime Navigation and Electronic Navigation

Navigation through the Strait of Hormuz is fundamentally dependent on automated digital coordination for shipping management. Vessels rely on systems such as the Automatic Identification System and Vessel Traffic Services to ensure safe transit and collision avoidance in one of the world's most congested maritime corridors. In the event of military escalation combined with disruption of subsea data links, the region would enter an information blackout and loss of situational awareness, thereby undermining its navigational reliability.

Recent data from maritime intelligence platforms such as Pole Star Global and MarineTraffic confirm that spoofing incidents affecting the Global Positioning System and interference with the Automatic Identification System within the Strait have already produced implausible and physically impossible vessel trajectories, including ships appearing to cover vast distances instantaneously or move along perfectly straight paths inconsistent with real navigation conditions. During peak disruption periods, Alphaliner documented that up to 65 container vessels simultaneously either deactivated their transponders or transmitted falsified geographic coordinates.

The severing of subsea data links would effectively isolate port authorities from real-time maritime activity and deprive shipping companies of their critical ability to monitor oil tankers and container vessels, verify their safety, and direct their movements with precision. In the absence of effective control, shipping operators would be forced to suspend operations entirely, leaving hundreds of vessels drifting in Gulf waters or anchoring in an unplanned manner. This, in turn, would significantly increase the likelihood of further accidental damage to submarine cables caused by anchor drag.

Port Operations and Customs Clearance

This informational and navigational disruption would have immediate and profound effects on operational processes within major transport hubs and ports, such as Jebel Ali Port in Dubai, where logistics operations are managed through advanced digital systems, including the Dubai Trade platform operated by DP World. These centralised systems process millions of electronic bills of lading, manage digital customs clearance procedures, and coordinate highly complex logistical algorithms governing container allocation and terminal operations. In the event of a severe disruption to data flows, major shipping companies would be unable to receive shipment data, complete customs procedures, or secure essential and immediate marine insurance coverage.

As a result, the movement of goods would come to a halt and supply chains would be disrupted, not because of a conventional physical or military blockade, but as the direct and inevitable consequence of a complete administrative and digital breakdown that halts international trade flows.

The safe operation of large tankers and modern container vessels depends entirely on the Automatic Identification System and continuous, real-time digital coordination with fleet command centres and port authorities. In the absence of submarine cable infrastructure linking regional port authorities to global shipping logistics networks, maritime traffic management and control would deteriorate into a highly unstable operational environment lacking even minimal levels of reliability.

These consequences have already been reflected in practice, as evidenced by the recent concentration of vessels in the Gulf of Oman and the open-ended suspension of navigation, following the refusal of commercial carriers to transit the Strait of Hormuz amid the simultaneous escalation of digital interference and heightened physical security concerns. This operational reality underscores that maritime stability and the security of trade in the region have become fully contingent on the integrity and continuity of digital infrastructure.

Geopolitical and Security Implications of Targeting Submarine Cables

Strategic calculations underpinning military operations in the Middle East are structurally and intrinsically linked to the integrity of civilian digital infrastructure. This interdependence is reflected in the heavy reliance of the United States military apparatus, particularly the United States Naval Forces Central Command and the Fifth Fleet based in the Kingdom of Bahrain, which plays a central role in securing the Strait of Hormuz and safeguarding global maritime routes, on commercial submarine cable networks to ensure effective logistical coordination and the management of intelligence-sharing systems.
Modern military operations require dense, continuous data flows, necessitating secure, high-capacity commercial fibre-optic routes to transmit vast volumes of intelligence, surveillance, and reconnaissance data, while also supporting cloud computing functions and directing unmanned aerial operations.

Contrary to the common assumption that modern militaries rely exclusively on closed, highly secure military satellite networks, the United States Department of Defense uses commercial fibre-optic routes to carry the majority of its high-bandwidth strategic communications. This dependence stems from the unmatched ability of submarine cables to provide exceptionally high data throughput, ultra-low latency, and cost efficiency, advantages that military satellite networks, whether operating in low Earth orbit or geostationary orbit, cannot match at comparable levels of operational performance.

Despite the presence of robust backup communication systems within military networks, the sudden loss of primary submarine fibre-optic routes would lead to a sharp degradation in situational awareness for deployed forces. This would significantly slow the real-time exchange of high-resolution geospatial intelligence and disrupt the transmission of large-scale telemetry data from unmanned systems, thereby impairing immediate operational coordination.

Such disruptions would compel military assets to shift to satellite communication links as a contingency measure, networks that are inherently congested and more vulnerable to advanced jamming techniques and intensive electronic warfare campaigns across Middle Eastern conflict theatres. In this context, the protection of submarine cables can no longer be regarded as a purely economic or commercial necessity. It has become a foundational pillar and a critical component of modern national security doctrine, extending across operational and strategic domains from outer space to the seabed.

Within the tactical balance of military and defence communications, the strategic exposure of the United States and its allies following the loss of terrestrial technological advantages coincides with the accelerated expansion of non-terrestrial operational capabilities by opposing actors. This shift is evident in the use by semi-military maritime militias of two-way short messaging services via dedicated frequency bands provided by China's BeiDou navigation satellite system, enabling these groups to maintain effective, autonomous operational coordination even when terrestrial networks are disrupted or compromised. Consequently, any disruption to submarine cables would directly erode the allied forces' terrestrial tactical superiority, forcing a shift toward congested, operationally vulnerable space-based assets, thereby increasing exposure to both security and operational risks.

The growing threat of targeting maritime infrastructure is driving a profound strategic shift, compelling both international and regional powers to reassess their defence policies and recalibrate existing deterrence frameworks. From a geopolitical perspective, data centres and submarine cable networks are increasingly being elevated to the status of sovereign strategic assets, comparable in criticality to nuclear facilities and conventional energy resources. This transformation is likely to incentivise military alliances to adopt more proactive and potentially pre-emptive doctrines, expanding their target sets to include the neutralisation of command and control centres and naval bases associated with threatening actors, such as Iran's Islamic Revolutionary Guard Corps.

Yet this trajectory of escalation is constrained by complex legal and operational challenges, particularly regarding the interpretation of Article 51 of the United Nations Charter. A central legal dilemma lies in the difficulty of classifying acts of economic sabotage as explicit armed aggression, thereby limiting the ability of affected states to invoke the right of self-defence. This ambiguity creates a legal grey zone that enables adversaries to conduct asymmetric disruptive operations while avoiding the threshold that would trigger comprehensive retaliatory military responses.

At the regional level, the strategic thinking and security doctrines of the Gulf Cooperation Council states are undergoing a fundamental shift toward greater self-reliance and independent initiative in securing maritime routes. Key states, notably Saudi Arabia and the United Arab Emirates, are integrating artificial intelligence, space-based surveillance, and unmanned aerial and maritime systems into comprehensive coastal defence architectures and operational protocols.

This advanced operational strategy is taking shape through targeted initiatives aimed at port protection, the deployment of precision maritime and satellite monitoring programmes, and the introduction of modern naval patrol vessels alongside specialised unmanned systems for mine-countermeasure operations to safeguard critical submarine cable routes. This evolving defence and technological posture is reinforced by intensified diplomatic efforts to build independent regional security alignments. Early signs of this trajectory are visible in ongoing strategic consultations aimed at formulating joint defence arrangements involving Riyadh, Islamabad, and Ankara, with the objective of establishing a security framework capable of protecting strategic communication lines from the volatility of external intervention.

In the context of long-term strategic and preventive responses to mitigate these risks, major global technology firms and cloud service providers are beginning to implement structural plans to re-engineer data flows and redirect them away from geopolitical hotspots and conflict-prone areas in the Middle East. These shifts are being operationalised through substantial capital investment in alternative transcontinental cable projects, most notably the "Waterworth" subsea cable, extending approximately 50,000 kilometres to connect the Americas, Africa, and Asia while fully bypassing the high-risk Red Sea corridor, alongside support for accelerated European initiatives to route critical communication lines through Arctic pathways.

In parallel with these commercial and technological efforts, major international institutions, including NATO and the European Commission, are adopting proactive and institutionalised defence approaches. These include the establishment of dedicated command centres focused exclusively on monitoring maritime infrastructure and assessing associated risks, as well as the implementation of stringent security and military protocols designed to ensure the resilience of critical networks and provide the necessary protection against emerging and asymmetric threats.

VII. Multidimensional Losses

The strategic repercussions of coordinated targeting of submarine communication cables across multiple nodes in the Middle East extend far beyond temporary technical disruption. They would instead generate a cascading macroeconomic contraction and an acute geopolitical crisis marked by the disruption of critical information flows and deep instability across the structure of global supply chains.

Macroeconomic and Financial Losses

A precise assessment of the substantial financial costs resulting from a regional internet disruption requires a systematic analysis of the degree of digital dependence within affected national economies. Based on analytical frameworks used by international institutions such as Deloitte and the Global Network Initiative, highly connected economies are estimated to lose approximately 1.9% of their daily gross domestic product for each day of severe or comprehensive internet disruption. In the context of Gulf Cooperation Council states, which exhibit some of the highest global rates of digital penetration and smart device usage, driven by long-term economic diversification strategies and Vision 2030 transformation agendas, applying this ratio to projected 2026 nominal GDP figures points to the prospect of massive daily financial losses. Such losses would be sufficient to generate rapid and structural imbalances in national fiscal frameworks.

Country	Nominal GDP (USD)	Estimated Daily GDP (USD)	Estimated Daily Loss at 1.9% (USD)
Saudi Arabia	1.3 trillion	3.6 billion	68.4 million
United Arab Emirates	601.2 billion	1.6 billion	31.1 million
Qatar	239.4 billion	655 million	12.4 million
Kuwait	162.9 billion	446 million	8.4 million
Oman	108.9 billion	298 million	5.6 million
Bahrain	49.2 billion	134 million	2.5 million

These quantitative estimates represent only a lower-bound, conservative approximation of the crisis. They capture direct losses from disrupted transactions and reduced productivity, but do not reflect the full scale of systemic and cumulative deterioration in capital markets driven by a sharp erosion of investor confidence.
Clear indicators of this financial risk have already emerged during periods of regional geopolitical tension, particularly during the escalation involving Iran, the United States, and Israel, when regulatory authorities in the United Arab Emirates were compelled to adopt pre-emptive measures, including the suspension of trading on the Dubai Financial Market and the Abu Dhabi Securities Exchange (ADX) for 48 consecutive hours to prevent panic-driven sell-offs.

Accordingly, any prolonged internet disruption, which would inevitably halt algorithmic and institutional trading, would necessitate the forced and open-ended closure of regional exchanges. This would freeze investor liquidity, fundamentally erode foreign capital confidence, and trigger substantial capital outflows from key financial centres such as Dubai and Bahrain, both of which have invested decades in establishing themselves as stable, secure, and reliable investment environments within the global financial system.

Logistical Disruptions and the Liquefied Natural Gas Supply Crisis

Disruptions to digital infrastructure act as a force multiplier of any physical logistical blockade. In the event of an actual closure of the Strait of Hormuz, whether resulting from the deployment of naval mines, the outbreak of direct military engagements, or digital failures affecting maritime coordination and customs clearance systems, global energy markets would face an immediate and severe structural deficit in liquefied natural gas supply. The scale of this strategic exposure is underscored by Qatar's market share, which accounts for approximately 20% of global supply, positioning it as a critical supplier for electricity generation in Europe and for sustaining major industrial economies in South Asia.

In this context, India relies on Qatari supplies for more than half of its liquefied natural gas imports, while Pakistan sources nearly all of its essential and strategic requirements from the same provider.

The persistence of this dual disruption, across both physical and digital dimensions, even for a matter of weeks, would generate acute price shocks, driving buyers in Europe and Asia into intensified competition within already volatile spot gas markets. Such dynamics would likely push spot prices to record levels exceeding $20 per million British thermal units.

These repercussions would compel countries such as India to implement immediate, stringent government measures to ration industrial gas consumption, leading to production shutdowns, jeopardising the fertiliser sector, which is critical to national food security, and placing severe strain on domestic power grids. The financial complexity of the crisis is further compounded by the fact that most long-term liquefied natural gas contracts are indexed to oil markets, with a pricing lag of approximately three months. As a result, the financial impact of such disruptions would continue to weigh on national energy budgets well beyond the restoration of physical maritime security.

In parallel, commercial fleets forced to exit the waters of the Strait of Hormuz or the Red Sea would be compelled to reroute via the Cape of Good Hope, an operational adjustment that adds between 10 and 14 days to each voyage. This collective geographic shift would sharply reduce global shipping capacity, trigger an immediate fourfold increase in maritime war-risk insurance premiums, and accelerate inflationary pressures across supply chains. The more acute challenge, however, would lie in the loss of stable digital connectivity. Container rerouting mechanisms would be disrupted, the issuance of electronic bills of lading would halt, and customs documentation processing in alternative ports such as Fujairah or Khorfakkan would be severely constrained. As a result, commercial cargo would remain stranded at sea, transforming routine maritime delays into a state of comprehensive logistical paralysis.

Geopolitical Exploitation, Information Vacuum, and Cyber Operations

Within the framework of modern hybrid warfare doctrine, the targeting of physical communication cables is not treated as an isolated tactical action, but rather as a foundational step that enables broader, multi-dimensional military and intelligence campaigns. The sudden destruction of this submerged infrastructure creates an immediate and comprehensive information blackout, which both state and non-state actors actively exploit to expand their operational influence.

During periods of severe network disruption, national and local authorities lose the ability to effectively disseminate emergency directives, while populations are abruptly cut off from reliable sources of information. This creates an environment highly conducive to large-scale psychological operations that amplify confusion and social instability, as demonstrated in recent Middle Eastern conflicts.

Simultaneously, state-aligned cyber groups, such as the "Handala Hack Team", exploit weakened network conditions by deploying ransomware, conducting sophisticated distributed denial-of-service attacks, and infiltrating operational systems within critical national infrastructure. Adversarial actors may also adopt tailored disruption strategies, including deliberate bandwidth-throttling techniques similar to Russia's "16-kilobyte curtain", which restricts access to internet infrastructure and digitally isolates users without resorting to a full network shutdown, thereby maximising psychological impact and institutional disruption.

Failure to secure critical digital corridors would constitute a strategic threat to the macroeconomic stability of Gulf Cooperation Council states, fundamentally undermining their geopolitical positioning as secure and reliable destinations for global technology investment. Should major technology firms such as Amazon, Google, and Meta conclude that geopolitical, security, and physical risks in the Middle East have exceeded manageable thresholds, they would likely move systematically to redesign their global network architectures and redirect future infrastructure investments away from the region altogether. Such a structural shift would risk isolating Gulf economies from the next generation of the global digital economy, inflicting significant damage on long-term strategic agendas aimed at achieving sustainable economic diversification.

Conclusion

Strategic maritime corridors in the Middle East, particularly the geographic expanse encompassing the Arabian Gulf, the Strait of Hormuz, and the Arabian Sea, represent the most critical geoeconomic convergence point between the physical flows of energy commodities and the digital movement of information within the global economy. While defence and economic analyses have historically focused on documenting the geopolitical vulnerabilities of these waterways in relation to the safe transit of crude oil and liquefied natural gas, a parallel security fragility lies beneath their contested depths.

This vulnerability is embodied in the dense geographic concentration of high-capacity submarine fibre-optic cable networks, which carry more than 95% of intercontinental communications and daily financial data flows. This concentration of immense data transmission capacity effectively transforms inherently narrow maritime corridors into highly sensitive structural chokepoints, posing a direct threat to the stability of the global digital economy.

In an international environment characterised by the intensification of hybrid warfare, escalating great-power competition, and the increasing militarisation of maritime domains, any deliberate and large-scale targeting of this submerged infrastructure would extend far beyond a localised disruption of communication services. It would constitute a multidimensional and catastrophic threat to global energy security, international financial stability, and regional geopolitical balances. Such coordinated disruption would generate a cascading and compound crisis, analytically definable as a dual-shock scenario, in which the paralysis of global energy supply chains coincides with a simultaneous and profound degradation of digital infrastructure across the Middle East, South Asia, and Europe.

Analytical modelling of this hypothetical sabotage scenario, grounded in the integration of historical precedents such as the Red Sea cable disruptions in 2024 with contemporary data on regional digital dependence, indicates that the destruction of communications infrastructure would constitute a severe structural shock to the global information economy. The direct financial losses resulting from such technical paralysis are estimated to reach hundreds of millions of dollars per day for Gulf Cooperation Council economies alone, accompanied by cascading disruptions affecting the stability of energy markets and financial settlement systems.

These repercussions extend far beyond the deprivation of consumer services. They encompass the paralysis of critical electronic clearing systems that underpin sovereign wealth fund investment operations, the disruption of digital command-and-control centres within state energy conglomerates, the impairment of military command-and-control networks, and the severance of essential communication channels required to manage and reroute maritime navigation during crises. Moreover, such sustained disruption would generate a geopolitical and security vacuum, one that has historically been exploited by both state and non-state actors to expand operational influence and advance disruptive agendas while evading effective deterrence or accountability.

As Middle Eastern economies accelerate their structural transition toward a development model centred on the digital economy and artificial intelligence, the region's economic trajectory has become fundamentally contingent on the resilience and strategic robustness of its maritime infrastructure. Mitigating this existential threat requires a fundamental shift in security doctrines and defence policies across regional governments and relevant international institutions, whereby submarine cable networks are accorded the same strategic priority and level of protection that has historically been reserved for crude oil pipelines and nuclear facilities.

This strategic shift also requires the mobilisation of substantial sovereign investment to establish parallel terrestrial backup routes and to accelerate the integration of advanced low Earth orbit satellite constellations as credible operational alternatives. In parallel, there is an urgent need to establish robust and well-equipped international maritime coalitions dedicated specifically to monitoring seabed environments and safeguarding data transmission corridors, with the aim of deterring acts of sabotage within so-called grey-zone conflict spaces. Absent the implementation of these comprehensive security and technological safeguards, global digital trade routes will remain acutely vulnerable, placing the entire international economic system at risk of an asymmetric shock of unprecedented scale and impact.

References

"A Houthi Undersea Capability." Strikepod Systems. February 23, 2024. https://www.strikepod.com/houthi-undersea-capability/.

"How Did We Survive the Red Sea Fiber Optic Cable Disaster How Did We Survive the Red Sea Fiber Optic Cable Disaster IPTP Networks." IPTP Networks | A Better Network, Not Just a Bigger One! (blog). June 12, 2025. https://www.iptp.net/blog/how-did-we-survive-the-red-sea-fiber-optic-cable-disaster/.

"Iran Submarine Capabilities Part of Submarine Proliferation Resource Collection." NTI. September 18, 2025. https://www.nti.org/analysis/articles/iran-submarine-capabilities/.

"New Iranian Weaponized Underwater Drone." Covert Shores. March 16, 2022. https://www.hisutton.com/Iran-IRGC-Weaponized-UUV.html.

"The Demise of Iranian Naval Power." The Australian Naval Institute. March 13, 2026. https://navalinstitute.com.au/the-demise-of-iranian-naval-power/.

"Undersea Sabotage Threatens Cables Connecting the World." The Cipher Brief. November 22, 2024. https://www.thecipherbrief.com/undersea-sabotage-threatens-cables-connecting-the-world.

Al Jazeera. "Internet Disruptions in Middle East and South Asia after Red Sea Cable Cuts." Al Jazeera, September 7, 2025. https://www.aljazeera.com/news/2025/9/7/internet-disruptions-in-middle-east-and-south-asia-after-red-sea-cable-cuts

Admin. "US DRONE HORROR: Iran's Stealth Undersea Killers Threaten US Carrier Strike Groups in the Persian Gulf Power Shift." Defence Security Asia. February 25, 2026. https://defencesecurityasia.com/en/us-drone-horror-iran-stealth-undersea-killers-threaten-us-carrier-strike-groups-persian-gulf/.

Aimé, Alex-Handrah, and Gaya Nagarajan. "Unlocking Global AI Potential with Next-generation Subsea Infrastructure." Engineering at Meta. February 14, 2025. https://engineering.fb.com/2025/02/14/connectivity/project-waterworth-ai-subsea-infrastructure/.

Alan Mauldin. "Navigating Hostile Waters: Submarine Cable Infrastructure and the Strait of Hormuz." TeleGeography. March 13, 2026. https://resources.telegeography.com/submarine-cable-infrastructure-strait-hormuz.
BusinessWorld. "India Cheap Internet Undersea Cable Vulnerability War Zones 2026." BusinessWorld, 2026. https://www.businessworld.in/article/india-cheap-internet-undersea-cable-vulnerability-war-zones-2026-598929

Chevalier, Franck, and Patrick Kidney. "Submarine Cable Security and Resilience." Analysys Mason. March 12, 2026. https://www.analysysmason.com/consulting/reports/submarine-cable-security-resilience/.

CXO TV / TechPlus Media. "Strait of Hormuz Crisis: Global Internet Cables at Risk as Oil Shipping Halt Sparks Fears of Worldwide IT Disruption." CXO TV, March 3, 2026. https://cxotv.techplusmedia.com/trending-news/strait-of-hormuz-crisis-global-internet-cables-at-risk-as-oil-shipping-halt-sparks-fears-of-worldwide-it-disruption

Çetikli, Deniz. Maritime Critical Infrastructure Protection (MCIP). Istanbul: Maritime Security Centre of Excellence (MARSEC COE), October 2023. https://www.marseccoe.org/wp-content/uploads/2023/10/Maritime-Critical-Infrastructure-Protection-.pdf

Coito, Joel. "Protecting Subsea Cables: Detect to Deter, Sue to Secure." Center for Strategic and International Studies (CSIS), December 12, 2025. https://www.csis.org/analysis/protecting-subsea-cables-detect-deter-sue-secure

Cory, Nigel, Matthew F. Ferraro, Justin B. Weiss, Emma Wright, and Caitlyn Weeks. "The Middle East's Big Bet on Artificial Intelligence and Data Security." Crowell & Moring LLP, September 24, 2025. https://www.crowell.com/en/insights/client-alerts/the-middle-easts-big-bet-on-artificial-intelligence-and-data-security

Desk, TOI T. "US-Iran War: Meta's Major Persian Gulf Cable Project Suspended." The Times of India. March 13, 2026. https://timesofindia.indiatimes.com/technology/tech-news/us-iran-war-metas-major-persian-gulf-cable-project-suspended/articleshow/129551761.cms.

Deloitte LLP. The Economic Impact of Disruptions to Internet Connectivity. Report prepared for Facebook Ireland Ltd. London: Deloitte LLP, October 2016. Hosted by Global Network Initiative. https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf

Dib, Diana, Imad Atwi, Prateek Chauhan, and Kirolous Zikry. "Smaller AI Models, Even Bigger Opportunity for the Middle East: Unlocking the Region's Potential in the AI Infrastructure Race." Strategy& Middle East, PwC Network, 2025. https://www.strategyand.pwc.com/m1/en/strategic-foresight/sector-strategies/technology/unlocking-the-ai-data-center-boom/ai-infrastructure-race.pdf

Dahm, J. Michael. "Undersea Fiber-Optic Cable and Satellite Communications." Johns Hopkins University Applied Physics Laboratory (JHU/APL), December 2022. https://www.jhuapl.edu/sites/default/files/2022-12/UnderseaFiber-OpticCableandSATCOM.pdf

Egeli, Sitki. "Threat From the Depths: Uncrewed Underwater Vehicles." Rabdan Security and Defence Institute. March 21, 2025. https://rsdi.ae/en/publications/threat-from-the-depths-uncrewed-underwater-vehicles.

Fraser, Iain. "Why GCC Oil & Gas Executives Must Treat SCADA & ICS Cybersecurity as a Strategic National Imperative." GeopoliticalMatters.com, November 18, 2025. https://geopoliticalmatters.com/2025/11/18/scada-and-ics-cybersecurity/

Farley, Robert. “The ‘Iran’s Navy Is Destroyed’ Narrative Is Missing a Huge Chunk of the Story.” 1945, March 8, 2026. https://www.19fortyfive.com/2026/03/the-irans-navy-is-destroyed-narrative-is-missing-a-huge-chunk-of-the-story/

Finance Middle East. "Can Banks Withstand Weeks of Disruption from Red Sea Cable Cuts?" Finance Middle East, 2025. https://www.financemiddleeast.com/banking-and-insurance/can-banks-withstand-weeks-of-disruption-from-red-sea-cable-cuts/

Farzin Nadimi. "The IRGC and the Persian Gulf Region in a Period of Contested Deterrence." Middle East Institute. November 3, 2021. https://mei.edu/publication/irgc-and-persian-gulf-region-period-contested-deterrence/.

Germond, Basil. "Critical Undersea Infrastructures: A Framework to Address Threats in a Post-Physical Context." Georgetown Journal of International Affairs. February 12, 2026. https://gjia.georgetown.edu/2026/02/12/critical-undersea-infrastructures-a-framework-to-address-threats-in-a-post-physical-context/.

Ghai, Gourav. "THREAT TO UNDERSEA INFRASTRUCTURE." CYFIRMA. April 2, 2024. https://www.cyfirma.com/blogs/threat-to-undersea-infrastructure/.

Giacomo Leccese. "Chokepoint Above and Below the Surface: The Red Sea's Emerging Infrastructure Challenge." IAI - Istituto Affari Internazionali. December 13, 2025. https://www.iai.it/en/publications/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge.

Hicks, Mike. "Diving Into the Red Sea Cable Cuts & More Outage News." CISCO Thousand eyes. September 19, 2025. https://www.thousandeyes.com/blog/internet-report-red-sea-subsea-cable-cuts.

Hendriks, Marcus Solarz, and Harry Halem. "From Space to Seabed: Protecting the UK's Undersea Cables from Hostile Actors." Policy Exchange, February 19, 2024. https://policyexchange.org.uk/publication/from-space-to-seabed/

Hunt, David. "Subsea Cable Sabotage: Underwater, Underprotected, and Under Attack!" Marine Technology News. December 9, 2025. https://www.marinetechnologynews.com/news/subsea-cable-sabotage-underwater-656389.

M. West, Darrell. "Global Economy Loses Billions from Internet Shutdowns." Brookings. October 24, 2016. https://www.brookings.edu/articles/paper-global-economy-loses-billions-from-internet-shutdowns/.

Monaghan, Sean, Michael Darrah, Eskil Jakobsen, and Otto Svendsen. "Red Sea Cable Damage Reveals Soft Underbelly of Global Economy." CSIS | Center for Strategic and International Studies. March 7, 2024. https://www.csis.org/analysis/red-sea-cable-damage-reveals-soft-underbelly-global-economy.

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

Morales, Jowi. "Iran Conflict Delays Meta's 2Africa Undersea Cable Project — Cable Layer Declares Force Majeure, Says It Can No Longer Safely Operate in the Persian Gulf." Tom's Hardware. March 13, 2026. https://www.tomshardware.com/tech-industry/iran-conflict-delays-metas-2africa-undersea-cable-project-cable-layer-declares-force-majeure-says-it-can-no-longer-safely-operate-in-the-persian-gulf.

Morales, Jowi. "Iran Conflict Delays Meta's 2Africa Undersea Cable Project — Cable Layer Declares Force Majeure, Says It Can No Longer Safely Operate in the Persian Gulf." Tom's Hardware. March 13, 2026. https://www.tomshardware.com/tech-industry/iran-conflict-delays-metas-2africa-undersea-cable-project-cable-layer-declares-force-majeure-says-it-can-no-longer-safely-operate-in-the-persian-gulf.

Phillip de Wet. "Iran Goes to War, but Red Sea Cables Not at Increased Risk." The Stack. March 2, 2026. https://www.thestack.technology/red-sea-cables-are-probably-safe-from-iran/.

Qiu, Winston. "War in the Gulf Severs the World's Digital Arteries: How the Iran Conflict Is Reshaping Global Connectivity." Submarine Networks. March 15, 2026. https://www.submarinenetworks.com/en/nv/insights/war-in-the-gulf-severs-the-world-s-digital-arteries.

Rishon, Makor, and Elie Klutstein. "The New Front Against Iran and Its Proxies: Underwater." Www.israelhayom.com. October 26, 2024. https://www.israelhayom.com/2024/10/26/the-new-front-against-iran-and-its-proxies-underwater/.

Thomas, Lynsey, and Eckhard Bruckschen. "UnderSea 2025 The Year the Subsea Cable Map Quietly Changed." InterGlobix Magazine. January 20, 2026. https://www.interglobixmagazine.com/undersea-2025-the-year-the-subsea-cable-map-quietly-changed/.

International Monetary Fund (IMF). "GDP, Current Prices (ARE, SAU, QAT, OMN, KWT, BHR)." World Economic Outlook Database, IMF Data Mapper. Washington, D.C.: International Monetary Fund, accessed March 2026. https://www.imf.org/external/datamapper/NGDPD@WEO/ARE/SAU/QAT/OMN/KWT/BHR

United States Department of State. "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World." U.S. Department of State, September 26, 2024. https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/

Investing.com. "Electronic Warfare Further Disrupts Shipping in Strait of Hormuz." Investing.com, 2026. https://ca.investing.com/news/economy-news/electronic-warfare-further-disrupts-shipping-in-strait-of-hormuz-93CH-4500429

Fortino, Kati. "Strait of Hormuz Disruption Impacts Global Logistics and Freight Networks." Customs Support, March 2, 2026. https://www.customssupport.com/strait-of-hormuz-impacts-global-logistics-and-freight-networks/

Gordon, Lori, and Karen Jones. "Global Communications Infrastructure: Undersea and Beyond." Center for Space Policy and Strategy (CSPS), Aerospace Corporation, February 1, 2022. https://csps.aerospace.org/sites/default/files/2022-02/Gordon-Jones_UnderseaCables_20220201.pdf

Risk Awareness. "War Risk to Global Data Corridors." Risk Awareness, 2025/2026. https://riskawareness.in/war-risk-to-global-data-corridors/

Varghese, Justin. "Iran War: Will Your Internet Slow Soon? Hormuz Tensions Raise Undersea Cable Risks." Gulf News, 2026. https://gulfnews.com/business/markets/iran-war-will-your-internet-slow-soon-hormuz-tensions-raise-undersea-cable-risks-1.500479198

Brookings Institution. "Protecting Underseas Cables." Brookings Institution, August 17, 2024. https://www.brookings.edu/articles/protecting-underseas-cables/

Runde, Daniel F., Erin L. Murphy, and Thomas Bryja. "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition." Center for Strategic and International Studies (CSIS), August 16, 2024. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Pidiha, Akshita. "Internet at Risk: War Zones Now Threaten Global Data Lifelines." Analytics Insight, 2025. https://www.analyticsinsight.net/news/internet-at-risk-war-zones-now-threaten-global-data-lifelines

Pidiha, Akshita. "Internet at Risk: War Zones Now Threaten Global Data Lifelines." Analytics Insight, 2025. https://www.analyticsinsight.net/news/internet-at-risk-war-zones-now-threaten

AL HABTOOR RESEARCH CENTRE

Strategic Estimates

About Al Habtoor Research Centre

Al Habtoor Research Centre strives to be a leading Centre of excellence for political studies, economics, and early warning in the region. Our vision is to foster informed and evidence-based policy and decision-making that promotes sustainable development, strengthens instutions and enhance regional peace and stability. We are committed to providing innovation solutions to the region's most pressing challenges through rigorous research, analysis, and dialogue.

Strategic Estimates

A non-periodic series issued by the Al Habtoor Research Centre, providing in-depth analysis and future assessments of regional and international political and economic issues with strategic impact on the Arab region and the world. It aims to provide decision-makers, researchers, and interested parties with an informed perspective on emerging developments, challenges, and opportunities.