Europe and Asia Facing Submarine Cable Disruption: Uneven Exposure and Alternative Routes

AL HABTOOR RESEARCH CENTRE

Strategic Estimates

October 2026

Submarine data cables have become a vital pillar for the security and economies of Europe and Asia, carrying the international data traffic that carries financial and commercial transactions, cloud computing and digital services, as well as cross-border business operations. The reliability of these services depends not only on the availability of functional cable systems but also on the geographical distribution of the routes connecting markets, data centres, and digital infrastructure.

In this context, the Red Sea region and the Bab el-Mandeb Strait are of particular significance. They link the Indian Ocean to the Mediterranean Sea and serve as a primary channel for data traffic between Asia and Europe. Furthermore, the risks in the Strait of Hormuz and Bab el-Mandeb raises the stakes for the submarine and terrestrial corridors connecting continents together. In such a context, countries including France, Italy, Germany, Pakistan, India, and Singapore face significant tests regarding their interconnectedness to such corridors. This raises crucial questions: how do countries differ in their ability to maintain connectivity, and what costs and dependencies do alternative routes introduce?

Which countries are Exposed, and why?

The level of risk, in terms of potential subsea cable disruptions, faced by France, Italy, Germany, India, Pakistan, and Singapore are determined by their position within international telecommunications networks, their reliance on specific transit corridors, and the availability of alternative routes.

The Red Sea region and the Bab al-Mandab Strait are of critical importance, as they form part of the primary data corridor connecting Europe and Asia via Egypt. Cable outages that occurred between February and March 2024, as well as a disruption in September 2025, demonstrated that damage to this corridor can affect connectivity efficiency across several countries. And with Iran's threats to target submarine cable in vital corridors, concerns are raised regarding European and Asian countries that could be affected.

A. France: High levels of international connectivity concentrated around Mediterranean gateways

France holds strategic importance as a key European entry point for subsea cables connecting Europe to the Middle East, South Asia, and Southeast Asia. The city of Marseille, in particular, stands out as a hub for numerous international cable systems, including "SEA-ME-WE 4" (SMW4), which connects Marseille, France and Palermo, Italy to countries in Asia and North Africa, including Singapore, Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, United Arab Emirates, Saudi Arabia, Egypt, Tunisia and Algeria. Also, "India–Middle East–Western Europe" (IMEWE), which connect France and Italy to India through the Middle East.

This dependency was clearly demonstrated during the disruptions of September 2025, when faults in the SMW4 and IMEWE systems near Jeddah led to a degradation in connectivity quality across several nations that rely on these networks. For France, the repercussions could extend to international internet traffic, access to cloud services, and various digital services that depend on connectivity to Asian markets.

Nevertheless, France's access to transatlantic cables and other European interconnection points provides alternative routes that can help mitigate its reliance on the Red Sea corridor. Consequently, the primary vulnerability doesn't lie in a lack of international connectivity, but rather in the concentration of Asia-bound traffic within Marseille, and the risk that multiple systems may share the same geographical bottlenecks.

B. Italy: Risks Posed by Submarine Cable Systems Linking the Mediterranean, Europe, and Asia

Italy faces a similar set of risks, as its international connectivity is integrated into the same Mediterranean networks that serve France and other European markets. Palermo serves as a landing point for the SMW4 cable system, and Italian operators participate in international cable systems that connect Europe to the Middle East and Asia.

Consequently, any disruption affecting the Red Sea segment of these systems could harm Italy's connectivity to Asian destinations, even if its domestic networks and other international links remain operational. Potential consequences may include slower access to external digital services, reduced performance for businesses transactions with Asian partners, and additional costs should data traffic need to be rerouted through alternative European or trans-Atlantic networks.

While Italy's location on the Mediterranean offers the advantage of access to numerous regional connections, geographical proximity to multiple cables doesn't guarantee service continuity if those cables share the same corridor. Similar to the case of France, the question arises as to whether Italy's available international routes and operator agreements provide sufficient independent capacity to maintain service in the event that major systems connecting to Asia are disrupted.

C. Germany: Indirect Exposure Through Reliance on Neighbouring Cable Hubs

Germany's exposure differs from that of France and Italy because it doesn't have the same level of direct connectivity through transcontinental submarine cables. The German Council on Foreign Relations (DGAP) explains that Germany relies on submarine cable infrastructure provided by other EU member states to connect to other continents.

It also points to the heavy concentration of cable systems between Europe and Asia along the Suez Canal and the Red Sea corridor.

Consequently, any disruption to this corridor could affect Germany through its reliance on international transit networks and landing points in other European countries, even if Germany's domestic telecommunications infrastructure remains intact. Companies that use international cloud computing platforms, financial services, and digital links with Asian markets could experience slower connections or higher transit costs if operators reroute data traffic through alternative paths.

Germany's extensive infrastructure of internet exchanges and domestic data centres supports internal connectivity but doesn't eliminate reliance on international routes. Therefore, Germany's resilience depends heavily on cross-border coordination, access to spare capacity in neighbouring networks, and the ability to reroute data traffic through transatlantic connections or other European gateways.

D. India: Extensive International Connectivity with Concentrated Landing Infrastructure and Reliance on Western Routes

India faces particularly significant risks, as its digital economy relies heavily on international connectivity to support IT services, software exports, financial operations, and cross-border business activities. India relies on 17 international subsea cable systems, with up to 14 landing stations distributed across five cities. This highlights a vulnerability to India if a long-term or simultaneous outage occurs. Another vulnerability revolves around the heavy concentration of landing infrastructure around Mumbai where landing points are concentrated at an access point spanning around six kilometres along Versova Beach.

Moreover, there is a critical importance of westward-bound cable systems, such as FALCON network, Gulf Bridge International system, SeaMeWe-6, and AAE-1, for India's connectivity with the Gulf region, Europe, and Africa. Hence, India's vulnerabilities stem from a combination of factors, including rising demand for international bandwidth, the concentration of landing-point infrastructure, and a reliance on western routes that could be compromised by disruptions in the Red Sea or the Gulf region.

The economic repercussions extend beyond general internet performance where India's substantial exports in information technology and business services rely on reliable connectivity with international clients, enterprise systems, and cloud infrastructure. While a disruption does not necessarily imply a total paralysis of these services, issues such as network congestion, increased latency, and reduced reliability can lead to breaches of service-level agreements and boost the costs of maintaining business continuity.

India most likely has more alternatives compared to countries with limited international connectivity; however, the availability of reserve capacity and the geographical independence of alternative routes remain critical factors. Furthermore, the operational status of new cable systems should be carefully verified that they are fully operational. In March, 2026, India's Ministry of Electronics and IT reported that the India Europe Xpress, SEA-ME-WE 6, and 2Africa cables were still under commissioning.

E. Pakistan: Heightened Vulnerability to Outages Amid Limited Alternatives

Pakistan's vulnerability to submarine cable failures is intensified by the fact that disruptions to international cables have previously compromised connectivity quality combined with the country's fewer available alternatives compared to those accessible to major European hubs. In other words, Pakistan's lack of alternatives has contributed to service degradation and access to global networks once disruptions occur.

Potential consequences include slower internet speeds, restricted access to offshore cloud computing platforms, and increased strain on telecommunications providers striving to maintain international bandwidth. These impacts are particularly significant for IT firms, software exporters, and other businesses that rely on dependable international connectivity. Nevertheless, Pakistan's vulnerability doesn't reflect an inevitable nationwide outage; instead, the severity of any disruption depends on which specific cable segments are affected, the remaining capacity available to operators, and the availability of independent routing paths.

The primary challenge for Pakistan likely lies in transforming additional cable connections into tangible resilience. Systems such as SEA-ME-WE 6 expand available connectivity options; however, their value during crises depends on the ability to bypass affected routes, the operational readiness of necessary components, and the availability of sufficient backup capacity. Hence, Pakistan's ability to manage outages will likely depend on expanding truly independent international routes, improving contingency arrangements among operators, and ensuring that backup capacity can be activated rapidly.

F. Singapore: An Extensive Telecommunications Network Subject to Shared Regional Bottleneck Risks

Singapore occupies a unique position; it serves as a major international telecommunications hub, connecting Southeast Asia to South Asia, the Middle East, Europe, and other global markets. Singapore has 26 submarine cables converge in three landing sites. This vast network allows Singapore to reroute data traffic across multiple systems gaining leverage over countries with limited international connectivity.

Singapore's links to Europe and the Middle East include cable systems that traverse the Indian Ocean and the Red Sea corridor. Consequently, a portion of the data traffic between Asia and Europe remains vulnerable to the same disruptions that could affect France, Italy, India, and Pakistan. Therefore, Singapore's connectivity advantage relies on the availability of alternative routes through other parts of Asia and across the Pacific Ocean.

Another vulnerability for Singapore lies in the concentration of its international telecommunications and data infrastructure within a relatively small geographical area. This means that having a large number of communication links doesn't necessarily guarantee immunity from risks associated with shared landing sites or regional bottlenecks. For Singapore, the central challenge is ensuring the continuity of connectivity for international businesses, cloud computing infrastructure, and regional data exchange in the event that multiple routes are disrupted simultaneously. While its extensive international links provide a significant leverage in terms of resilience, this leverage is conditioned in terms of route overlap, the distribution of landing infrastructure, and the capacity available across alternative paths.

Economic Consequences of Submarine Cable Disruptions

Submarine cable disruption would affect economies not simply by reducing internet access, but by raising the cost, delay and uncertainty of moving data across borders. The exposure is structural: over 90% of Europe–Asia capacity is carried by Red Sea cables, and over half of many countries' interregional bandwidth reaches Europe by the same route. A country would not necessarily suffer a nationwide blackout; domestic networks could keep working while international cloud services, financial transactions and business communications become slower or less reliable. Rerouting works, but it costs time: after the September 2025 cuts near Jeddah, Europe–Mumbai latency rose from about 110–150 ms to 190–300 ms, with rerouting often adding 50–100 ms. Published loss estimates for the 2024 and 2025 episodes remain scarce, so this section assesses exposure rather than measuring damage.

The financial services sector is one of the most exposed sectors, as they are particularly sensitive to connectivity disruptions because banks depend on reliable communications for international payments, interbank transfers, trading platforms and access to external financial infrastructure, SWIFT averaged 44.8 million messages a day in 2022, transmitted over undersea cables. Payment messaging can tolerate some delay, but trading platforms, real-time APIs and risk systems are far less forgiving of latency spikes. France, Germany and Italy would feel this through institutions reliant on Asia-linked data exchange, with Germany exposed indirectly through neighbouring cable gateways. Singapore's role as a financial centre makes connectivity to global hubs especially important. Impact depends on which routes fail, not on cable counts.

IT and outsourcing face a different problem: dependence on real-time links to overseas clients. India, as the previous section showed, combines concentrated landing infrastructure with heavy reliance on westbound routes. When Europe–Mumbai latency nearly doubles, costs appear in video calls, remote desktops and ERP systems rather than an outage, consistent with the minister's statement that India's systems were "not critically impacted" in 2025. A severe outage could delay software delivery and customer support; the Observer Research Foundation estimates losses as high as US$920 million on India's IT and services economy from a 24-hour internet disruption, a measure of exposure, not a forecast. Pakistan's outsourcing firms face similar risks with fewer alternatives; after the January 2025 AAE-1 fault, officials reported recovering about 80% of the shortfall by shifting traffic to two other cables.

Logistics is exposed through data rather than cargo. Every shipment carries metadata that moves it through customs clearance and enables tracking. Degraded links would more likely slow clearance, weaken visibility and raise the cost of exceptions than halt trade, with time-sensitive and just-in-time consignments bearing the heaviest burden.

Europe's exposure runs through its gateways. Marseille hosts 17 cable landings and Sicily more than 20, so a corridor failure would concentrate pressure on a few French and Italian hubs even where end users notice little change, while Germany depends on its neighbours' infrastructure. The effects would not be uniform across countries or businesses.

Uneven Exposure: Economic Activities and Cable Dependencies by Country

Country	Economic activities exposed	Principal concern
France	Financial services, cloud, international business, logistics	Costlier, less reliable Europe–Asia data exchange
Germany	Industrial supply chains, enterprise IT, finance	Delays in cross-border data supporting production
Italy	Telecoms, finance, logistics	Disruption at Mediterranean landings and onward links
India	IT services, outsourcing, finance	Overseas client services and business continuity
Pakistan	Digital services, outsourcing, finance	Deeper degradation where alternatives are scarce
Singapore	Finance, maritime logistics, cloud	Time-sensitive, high-volume connectivity

Table: Al Habtoor Research Centre • Source: Various Sources • Created with Datawrapper

The greatest costs would fall on firms with real-time cross-continental dependencies and little route diversity: financial institutions running Europe–Asia trading and settlement links, outsourcing exporters serving European clients, and smaller companies without multi-carrier or multi-region cloud arrangements. Short outages may be manageable where backup capacity suffices; prolonged ones risk missed transactions, contractual penalties and eroding confidence. The impact ultimately depends on sectoral exposure, alternative capacity and recovery speed.

Alternative Routes and Connectivity Options by Country

Alternatives exist, but none can quickly replace the Red Sea. TeleGeography notes that India has links eastward to Singapore, yet warns that you cannot quickly and completely reroute all existing traffic along other paths. The practical question, following the exposure patterns outlined above, is which options are operational today and which countries can reach them. Surviving corridor cables are the fastest response. After the January 2025 AAE-1 fault, Pakistan's IT minister said around 80% of the bandwidth shortfall had been recovered by shifting traffic to two other cables. The limit is correlation: in 2025, AAE-1 and PEACE were disrupted simultaneously, hurting Asia–Europe capacity. This works for a limited cut, not a corridor failure.

Routes around Africa or through the United States exist but are longer and costlier, and new capacity is still arriving. India's Ministry of Electronics and IT reported in March 2026 that India Europe Xpress, SEA-ME-WE 6 and 2Africa were still under commissioning. Eastbound routing is proven: traffic was rerouted east through Singapore and onward to the US in earlier disruptions, supported by transpacific systems such as Echo and Bifrost. France and Italy can also use Atlantic routes, but US hyperscalers already own 90% of capacity on the US–Europe cable route, according to the EU's expert group, a dependency with its own political cost.

Overland Eurasian options are mostly planned or unproven, the Trans-Caspian cable's subsea section was completed on 6 October 2026, with capacity above 400 Tbps, but a working corridor requires sufficient terrestrial capacity in Azerbaijan, Georgia and Kazakhstan and commercial agreements between operators. The northern route through Russia is described as sanctioned. Iraq's Ooredoo contract, signed on 10 September, was expected to take three to four months.

Timelines separate the options. Rerouting onto surviving cables can take hours to days, as in Pakistan's case; repairs take weeks to months, with PEACE restored in three weeks in 2025 but Red Sea repairs in 2024 taking up to five months; new systems and overland corridors take months to years, and many remain unproven.

Alternative Routes: Status and Constraints

Option	Status	Main constraint
Surviving corridor cables	Operational	Correlated failure; slow repair
Around Africa	Existing, longer	Latency, cost, delayed builds
Via Singapore and the US	Operational	Distance; hyperscaler dependence
Trans-Caspian corridor	Newly built	Terrestrial links, agreements
Iraq–Türkiye route	Under construction	Security; completion timing

Only the first three are operational today; the Trans-Caspian and Iraqi corridors are newly built or still under construction.

Table: Al Habtoor Research Centre • Created with Datawrapper

Authors' analytical framework, reproduced from the supplied manuscript.

Political constraints bind as tightly as technical ones. Gulf-based alternatives inherit the Hormuz risk, since the IRGC has threatened to target subsea cables there. Cost evidence is thinner: sources call alternatives longer and more expensive but rarely quantify the premium.

Access therefore differs by country. France and Italy are best placed, combining Mediterranean landings with Atlantic and European interconnection points; Germany reaches these routes through neighbouring gateways and depends on cross-border coordination. Singapore's 26 cables, against India's 17, give it more rerouting options, though its Europe-bound paths still cross the corridor. India has more alternatives than Pakistan, but spare capacity and route independence remain decisive. Pakistan has the fewest credible options: PEACE and SEA-ME-WE 6 expand its choices, yet a link sharing the Red Sea corridor offers little protection, and PEACE itself was hit by a Red Sea outage in March 2025.

Each option should be tested against the questions raised earlier: is it independent of the corridor, how much traffic can it carry, and which services can tolerate its latency and cost? The surest alternatives are those already built, and the most promising are those not yet finished. Which countries will complete theirs before the corridor next fails?

What Are the Alternative Scenarios?

The consequences of submarine cable disruption depend on two interrelated factors, the duration of the outage and the availability of alternative transmission capacity. A cable failure does not automatically cause a nationwide internet blackout. Telecommunications operators can redirect traffic through surviving cables and terrestrial networks, but the effectiveness of these measures depends on spare capacity, existing agreements, and the independence of alternative routes.

The February 2024 Red Sea cable damage illustrates this vulnerability. The incident initially affected an estimated 25% of data traffic between Asia, Europe, and the Middle East, requiring operators to reroute traffic through surviving connections. The experience demonstrated that connectivity could be maintained despite significant damage, but also exposed the limits of alternative capacity. Four scenarios illustrate how different combinations of outage duration and available alternatives could shape the economic consequences.

Scenario One: Short Disruption with Sufficient Alternative Capacity

In this scenario, damage to several cables causes temporary service degradation, but surviving systems absorb most displaced traffic. Operators activate existing contingency arrangements, redirecting data through unaffected connections and alternative gateways. Most users experience limited disruption, although longer transmission routes may increase latency, the time required for data to travel between two points.

France, Germany, and Italy could draw on alternative European and transatlantic connections, while Singapore could benefit from its extensive regional connectivity. India and Pakistan would depend on the availability of alternative international gateways and sufficient capacity to accommodate westward traffic. Nevertheless, national connectivity advantages should not be confused with guaranteed resilience. A country may have numerous cables but remain exposed if its operators depend on the same maritime corridor.

Financial transactions, cloud services, and logistics platforms would largely remain operational, although applications requiring rapid data exchange could experience slower performance. The immediate priority would be to monitor network conditions, activate rerouting arrangements, and protect capacity for essential services. Under these conditions, disruption would remain primarily an operational challenge rather than develop into a prolonged economic shock.

Scenario Two: Short Disruption with Insufficient Alternative Capacity

A more difficult outcome would emerge if several cables failed simultaneously while surviving routes lacked sufficient spare capacity. Congestion, slower transfers, and intermittent access to international platforms could occur even if the outage lasted only a few days.

India and Pakistan could face pressure on financial services, cloud-dependent businesses, and IT outsourcing operations serving overseas clients. Singapore's role as a regional digital hub could expose businesses handling international data transfers to congestion. European firms could also experience delays when communicating with Asian offices, processing transactions, or accessing cloud services hosted abroad.

However, disruption would vary by provider, destination, and application. Domestic services and locally hosted content could remain accessible even as international platforms deteriorated. Businesses dependent on real-time transactions or continuous data exchange would face greater costs than those able to postpone non-essential transfers.

Operators would need to prioritise essential traffic, purchase additional capacity where available, and coordinate with other carriers. Governments and regulators should facilitate emergency arrangements while ensuring that limited capacity is allocated transparently. The principal challenge would be securing sufficient usable bandwidth, rather than simply identifying alternative cables.

Scenario Three: Prolonged Disruption with Sufficient Alternative Capacity

A prolonged outage would become more manageable if alternative routes could sustain essential traffic for weeks or months. Connections around Africa, across the Atlantic, through other Mediterranean gateways, and along operational overland Eurasian networks could provide additional options. However, these alternatives differ in capacity, latency, cost, and political accessibility.

European countries would generally have greater opportunities to distribute traffic across different international corridors, although individual operators and Asia-bound services could remain exposed. Singapore and India could redirect selected traffic through alternative Asian or Pacific connections, depending on destination and available capacity. Pakistan's options would depend on its international gateways and the capacity of neighbouring terrestrial networks.

Essential financial transactions, government communications, and logistics services could continue operating, but businesses might incur higher transit costs and reduced performance. IT outsourcing firms would face particular pressure where contractual obligations require reliable connections to overseas clients. Logistics companies could encounter delays in exchanging data among ports, shipping operators, customs authorities, and international customers.

The central risk would be the cumulative cost of maintaining connectivity through less efficient routes. Operators would need additional capacity agreements and geographically diverse pathways, while governments would need to facilitate cross-border transit arrangements. Prolonged resilience would therefore depend on commercial agreements and political cooperation established before disruption occurs.

Scenario Four: Prolonged Disruption with Limited Alternatives

The most severe scenario would combine extensive cable damage with insufficient alternative capacity, delayed repairs, or restrictions on transit through alternative territories. Congestion could persist, replacement capacity could become more expensive, and some international services could remain unreliable for an extended period.

India and Pakistan could face considerable pressure if their westward traffic could not be redirected at sufficient scale. Singapore's position as a regional digital hub could transmit disruption to businesses serving neighbouring markets. France, Germany, and Italy would retain alternative international connections, but services dependent on particular Asia-bound routes could still experience delays and higher costs.

Repair timelines would intensify these pressures. The International Telecommunication Union (ITU) notes that repairs can take from two weeks to several months, depending on location, weather, and procedural obstacles. Security restrictions and delays in obtaining permits could further extend outages in sensitive maritime areas.

Governments would need to coordinate continuity arrangements for essential financial, energy, telecommunications, and logistics services. Businesses would have to prioritise critical workloads, use alternative hosting environments where feasible, and prepare for sustained increases in connectivity costs. Ultimately, resilience would depend not simply on the existence of alternative routes, but on their independence, capacity, accessibility, and ability to remain operational during a regional crisis.

What Should Governments and Companies Prioritise?

The four scenarios demonstrate that connectivity resilience requires preparation before disruption occurs. Governments can reduce avoidable regulatory obstacles, encourage investment in independent routes, and coordinate emergency responses. Telecommunications operators and businesses must translate these measures into practical continuity arrangements. Priorities should reflect the different vulnerabilities of France, Germany, Italy, India, Pakistan, and Singapore rather than assume that all six countries face identical risks.

Strengthening Immediate Continuity Measures

First, governments should establish coordinated procedures for major international connectivity disruptions. Telecommunications regulators, national cybersecurity authorities, and network operators should maintain assessments of cable dependencies, alternative routes, available capacity, and critical services. These assessments should identify the connections supporting essential financial transactions, government communications, energy operations, cloud services, and logistics.

Second, operators should test whether backup arrangements can accommodate simultaneous cable failures rather than isolated outages. Several cables do not necessarily provide meaningful redundancy if they pass through the same maritime chokepoint or depend on the same landing station. Operators should therefore assess the complete transmission pathway, including terrestrial backhaul and onward international connections. They should also negotiate capacity agreements with multiple carriers and conduct realistic rerouting exercises.

Third, governments and businesses should establish transparent priorities for allocating limited capacity during severe disruption. Essential financial settlement, emergency communications, energy operations, and public services may require stronger continuity guarantees than non-critical data transfers. Businesses should identify applications that can temporarily operate at reduced performance or defer data transfers, preserving bandwidth for activities that cannot be interrupted.

These measures are particularly important for India and Pakistan, where pressure on international routes could affect businesses and users at scale. Singapore should test contingency arrangements with international carriers, while France, Germany, and Italy should assess exposure at the level of individual operators and Asia-bound services rather than relying on Europe's overall connectivity as evidence of resilience.

Diversifying Routes and Reducing Structural Dependencies

Over the longer term, governments should encourage investment in geographically diverse international connections. Routes around Africa could reduce reliance on the Red Sea, Bab el-Mandeb, and Egypt, while alternative Mediterranean connections could provide additional options for selected traffic flows. Operational overland Eurasian fibre networks could also contribute to diversification, subject to cross-border agreements and political conditions.

However, these alternatives are not interchangeable. Routes around Africa may increase transmission distances and costs, while terrestrial networks depend on transit permissions, infrastructure availability, and the security of countries along their pathways. Proposed cables and planned corridors should not be counted as operational redundancy until construction, connections, and commercial capacity arrangements are complete.

For France, Germany, and Italy, European Union coordination offers a framework for identifying shared vulnerabilities and directing investment towards critical gaps. In February 2026, the European Commission announced €347 million for strategic submarine cable projects, including €20 million dedicated to strengthening repair capacity. These measures provide a basis for improving European preparedness, although their effectiveness will depend on implementation and the operational independence of the resulting infrastructure.

India should strengthen international route diversity and assess whether alternative westward and eastward connections can absorb significant traffic transfers. Pakistan should prioritise independent international gateways, feasible regional terrestrial connections, and arrangements that reduce reliance on a limited number of systems. Singapore should continue diversifying its international connections while ensuring that new routes offer genuine geographic separation and sufficient capacity during simultaneous failures.

Improving Repair Readiness and Business Continuity

Infrastructure diversification must be accompanied by faster repair arrangements. Governments should streamline emergency permits, coordinate with neighbouring coastal states, and establish procedures for repair vessels to operate safely in affected waters. Cable operators should maintain repair agreements, access to specialised vessels and spare equipment, and mechanisms for coordinating restoration. These measures are particularly relevant to the Red Sea, where security conditions and administrative restrictions can complicate repairs.

At the corporate level, financial institutions, cloud service providers, IT outsourcing firms, and logistics companies should map their dependence on international connectivity providers. They should identify critical applications, test alternative network arrangements, and determine which services can operate through geographically separate data centres. However, geographic separation alone is insufficient if both locations ultimately depend on the same cable corridor.

Finally, governments and operators should conduct joint exercises simulating short outages and prolonged disruption. These exercises should test alternative routing, capacity availability, customer communications, and repair coordination. Their findings should guide investment and continuity planning.

Ultimately, the most resilient countries will not necessarily be those with the greatest number of cables, but those able to maintain essential services when several connections fail simultaneously. Geographic diversity, sufficient spare capacity, rapid repairs, and effective coordination will determine whether disruption remains a manageable technical problem or develops into a wider economic shock.

Conclusion

The ability to maintain connectivity upon disruptions in the Red Sea and the Bab el-Mandeb Strait depends less on the number of cables a country possesses, and more on the availability of geographically diverse routes, sufficient spare capacity, and the ability to access alternative networks without carrying the burden of expensive costs or creating new strategic dependencies.

France, Italy, Germany, India, Pakistan, and Singapore occupy distinct positions within the global network and would likely face varying constraints if the primary corridor face disruptions. France and Singapore may be relatively well-positioned compared to other countries while Germany and Pakistan face a certain challenge in being dependent on neighbouring countries for access to major international subsea cable systems.

Consequently, the existence of a single alternative capable of fully replacing the Red Sea corridor in every disruption scenario could be far unlikely. The most realistic strategy could likely be a multi-layered approach that combines the immediate rerouting of data traffic, the provision of additional independent international routes, and measures to reduce reliance on vulnerable transit points.

Alternative corridors may help reduce reliance on the Bab El-Mandeb cable; however, their effectiveness depends on operational readiness, cross-border accessibility, cross-border agreements, and the extent to which they can overcome other vulnerable regional chokepoints. Hence, a combination of leveraging existing rerouting capabilities, investing in geographically independent infrastructure, enhancing repair readiness, and developing coordinated contingency plans could offer a pragmatic resilient strategy.

References

Bashfield, Samuel, et al. 2026. “Rewiring the Indian Ocean: The Dynamic Geography of Submarine Cable Networks.” Australian Journal of Maritime & Ocean Affairs, August, 1–20. https://doi.org/10.1080/18366503.2026.2704274.

Beckman, Robert C., et al. “Enhancing the Security of Singapore’s Submarine Cables: Strengths, Challenges and Opportunities.” RSIS, May 21, 2024. https://rsis.edu.sg/rsis-publication/cens/enhancing-the-security-of-singapores-submarine-cables-strengths-challenges-and-opportunities/.

Bueger, Christian, et al. “Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU.” European Parliament, January 6, 2022. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf.

Chege, Kevin. “What Can We Learn from Africa’s Multiple Submarine Cable Outages?” Internet Society Pulse, August 6, 2024. https://pulse.internetsociety.org/en/blog/2024/08/what-can-we-learn-from-africas-multiple-submarine-cable-outages/.

Debates, Raisina. “Undersea Chokepoints: The Red Sea Cable Disruptions.” Observer Research Foundation, May 21, 2024. https://www.orfonline.org/expert-speak/undersea-chokepoints-the-red-sea-cable-disruptions.

European Commission. “Report on Security and Resilience of EU Submarine Cable Infrastructures.” Shaping Europe’s Digital Future, October 23, 2025. https://digital-strategy.ec.europa.eu/en/library/report-security-and-resilience-eu-submarine-cable-infrastructures.

European Commission. “Security and Resilience of EU Submarine Cable Infrastructures: Mapping, Risk Assessments, Stress Tests.” October 2025. https://table.media/assets/europe/submarine_cables_expert_group_mapping_risks_stress_tests_annex_fyjj1zl1m3ncdevktv9egwjld8_120905.pdf.

European Commission. “Submarine Cable Security Toolbox and Cable Projects of European Interest.” Shaping Europe’s Digital Future, February 5, 2026. https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest.

Euronews and Associated Press. “What Do We Know about Internet Disruptions from Cut Subsea Cables in the Red Sea?” Euronews, September 8, 2025. https://www.euronews.com/2025/09/08/what-do-we-know-about-internet-disruptions-from-cut-subsea-cables-in-the-red-sea.

Gambrell, Jon. “Commercial Shipping Likely Cut Red Sea Cables That Disrupted Internet Access, Experts Say.” Associated Press, September 9, 2025. https://apnews.com/article/red-sea-undersea-cables-cut-internet-disruption-0b08fc5f02daf72710e0010c11ea21ae.

Hartmann, Jannik. “Protecting the EU’s Submarine Cable Infrastructure.” German Council on Foreign Relations (DGAP), July 10, 2023. https://dgap.org/en/research/publications/protecting-eus-submarine-cable-infrastructure.

“India.” Submarine Cable Networks. Accessed October 22, 2026. https://www.submarinenetworks.com/en/stations/asia/india.

Internet Society. “Policy Brief: Enhancing the Resilience of Submarine Internet Infrastructure.” December 4, 2025. https://www.internetsociety.org/resources/policybriefs/2025/enhancing-the-resilience-of-submarine-internet-infrastructure.

ITU. “International Advisory Body Approves Landmark Report to Strengthen Submarine Cable Resilience.” July 10, 2026. https://www.itu.int/en/mediacentre/Pages/PR-2026-07-10-Submarine-cable-resilience-report.aspx.

Jagtiani, Sharinee L. “Risky Configuration: China’s Footprint in Germany’s Technology Stack.” German Marshall Fund of the United States, September 2025. https://www.gmfus.org/sites/default/files/2025-09/Germany%20Tech%20Stack_0.pdf.

Jainendran, Pranoy. “The Undersea Front: Iran’s Cable Threat and India’s Digital Vulnerability.” Observer Research Foundation. Accessed October 22, 2026. https://www.orfonline.org/english/expert-speak/the-undersea-front-iran-s-cable-threat-and-india-s-digital-vulnerability.

Khanna, Monty. “A Roadmap for Securing India’s Undersea Cables.” Observer Research Foundation, June 27, 2025. https://www.orfonline.org/research/a-roadmap-for-securing-india-s-undersea-cables.

Leccese, Giacomo. “Chokepoint Above and Below the Surface: The Red Sea’s Emerging Infrastructure Challenge.” Italian Institute for International Political Studies (IAI), December 13, 2025. https://www.iai.it/en/publications/c41/chokepoint-above-and-below-surface-red-seas-emerging-infrastructure-challenge.

Ministry of Electronics and Information Technology. “Data Centre Capacity in the Country Has Grown from 375 MW in 2020 to More than 1500 MW.” Government of India, March 18, 2026. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241783&lang=1&reg=6.

Murphy, Erin L., and Thomas Bryja. “The Strategic Future of Subsea Cables: Egypt Case Study.” Center for Strategic and International Studies, November 12, 2025. https://www.csis.org/analysis/strategic-future-subsea-cables-egypt-case-study.

Murphy, Erin L., and Thomas Bryja. “The Strategic Future of Subsea Cables: Singapore Case Study.” Center for Strategic and International Studies, September 24, 2025. Updated October 28, 2025. https://www.csis.org/analysis/strategic-future-subsea-cables-singapore-case-study.

“Peace.” Submarine Cable Networks. Accessed October 22, 2026. https://www.submarinenetworks.com/en/systems/asia-europe-africa/peace.

Patil, Sameer. “Undersea Chokepoints: The Red Sea Cable Disruptions.” Observer Research Foundation, May 21, 2024. https://www.orfonline.org/expert-speak/undersea-chokepoints-the-red-sea-cable-disruptions.

“Press Release PR No. 232.” Press Information Department, Ministry of Information and Broadcasting, Government of Pakistan, November 22, 2025. https://pid.gov.pk/site/press_detail/31076.

Sector, Development. Global Connectivity Report 2025. International Telecommunication Union, 2025. https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICT_MDD.GCR-2025-4-PDF-E.pdf.

“SEA-ME-WE 4.” Submarine Cable Networks. Accessed October 22, 2026. https://www.submarinenetworks.com/en/systems/asia-europe-africa/smw4.

“Submarine Cable Map.” TeleGeography. Accessed October 22, 2026. https://www.submarinecablemap.com/.

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.