Uncertainty is the New Normal

Is your network built to endure?

Enterprises today are operating in a world where uncertainty is no longer episodic, it is constant. Ongoing conflicts and regional wars, coupled with geopolitical tensions, shifting trade corridors, regulatory fragmentation, and macroeconomic volatility, are actively reshaping how global networks behave What was once considered stable global infrastructure is now increasingly prone to disruption, exposing enterprises to systemic risks across their digital infrastructure including connectivity, cloud, data centres, and critical workloads.

A significant share of global internet traffic continues to flow through a few highly concentrated chokepoints, amplifying this risk.

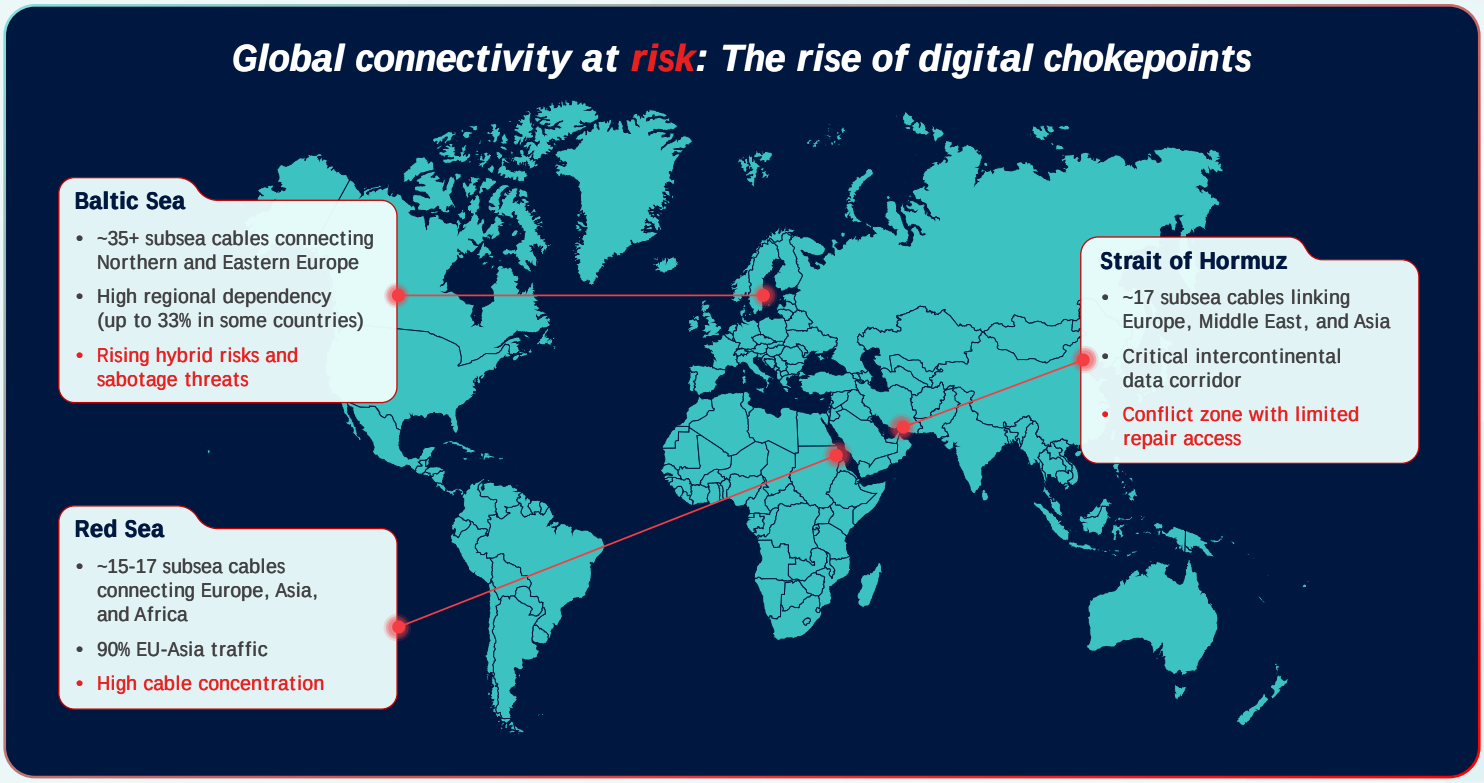
Egypt alone carries around 17% of global traffic, with over 90% of Europe–Asia data flows transiting through the Red Sea corridor. The vulnerability of this concentration was evident in March 2024, when multiple subsea cable cuts in the region disrupted nearly 25% of telecommunications traffic between Asia, Europe, and Africa, triggering widespread outages[1]. For organisations with cross-border operations, these are not abstract risks, they directly impact the reliability, performance, and security of critical workloads.

At the same time, enterprises are scaling AI-driven and digital workloads that depend on continuous, high-performance connectivity between geographically distributed data centres. This convergence of rising dependency and rising uncertainty is creating a new challenge: ensuring business continuity when the underlying network itself is exposed to disruption.

Connectivity is no longer neutral, it is being contested

What is changing now is not just the frequency of disruptions, but the nature of control over connectivity itself. In a world shaped by geopolitical competition, connectivity is increasingly emerging as an attack vector and at times, even a strategic lever in both physical and cyber warfare.

Today, the physical backbone of global networks is under growing strain across multiple high-risk zones.



In the Baltic Sea, a series of subsea cable disruptions, often occurring in clusters and under unclear or contested circumstances, has raised concerns around potential sabotage and "hybrid" threats. In 2024 alone, multiple cuts to cables between Finland/Germany and Sweden/Lithuania were reported, with at least 11 disruptions over ~15 months[2]. For countries like Lithuania, where up to 33% of internet capacity depends on these routes, the exposure is significant[3].

Further south, the Red Sea corridor continues to represent one of the world's most critical and vulnerable data highways, carrying the majority of Europe–Asia traffic. Past disruptions in this region have already demonstrated how a single incident can cascade into widespread latency spikes, rerouting, and service degradation across continents.

At the same time, the Strait of Hormuz is emerging as a new high-risk digital choke point. With ~17 subsea cables tightly clustered in a narrow passage, it forms a critical bridge between Europe, the Middle East, and Asia[4]. In a region now impacted by active conflict, the risks extend beyond physical damage to include restricted repair access, prolonged outages, and systemic disruption to global data flows.

Together, these developments underline a fundamental reality: connectivity is no longer inherently always-on, neutral, or guaranteed. It can be disrupted physically, constrained digitally, or influenced strategically.

A strategic shift: From just performance to complete resilience

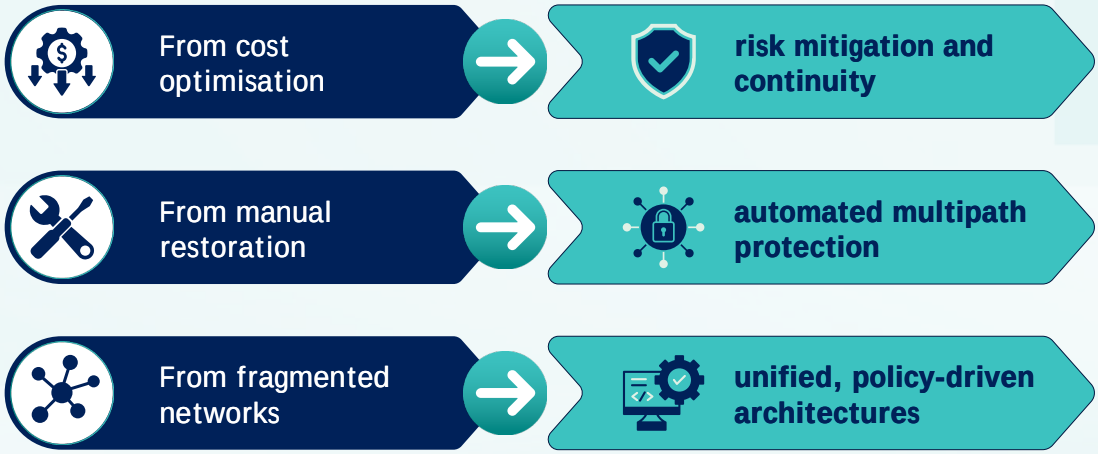
In response, enterprises are rethinking their priorities. The conversation is no longer centered on bandwidth or cost alone; it is increasingly about resilience and assured continuity. Organisations are actively reassessing how they connect data centres globally, with a sharper focus on:

- Redundancy across multiple routes and geographies
- Consistent performance for critical workloads
- Automated path restoration to avoid delays
- End-to-End visibility and control over cross-border traffic

This marks a fundamental shift from considering connectivity just as a utility to a strategic safeguard. The goal is not just to move data, but to ensure that data can move securely, predictably, and without disruption, regardless of external conditions.

Resilience is the new competitive edge

As global uncertainties continue to intensify, enterprises with cross-border operations and critical workloads, the ability to anticipate, adapt, and recover from disruptions will define success in the AI era. To ensure this, organisations are moving:



The mandate is clear: move beyond traditional connectivity and invest in resilient, intelligent Data Centre-to-Data Centre networks that ensure business continuity, no matter the conditions.

In an unpredictable world, the question is no longer whether disruptions will occur, it is whether your network is built to withstand them.

About Tata Communications

Tata Communications delivers networks that can anticipate, absorb, and recover from disruptions in real time while consistently ensuring low-latency performance for AI-driven and real-time applications. With 500,000+ km of subsea fibre, 200,000+ km of terrestrial network, and reach across 190+ countries, it provides inherent route diversity and geographic redundancy to mitigate regional and geopolitical disruptions. Its self-healing capabilities such as automated failover and intelligent path control enable enterprises to dynamically reroute traffic, isolate failures, and maintain application availability during network or infrastructure disruptions by building robust Data Centre-to-Data Centre connectivity globally. By combining global scale with intelligent control and built-in redundancy, Tata Communications enables enterprises to move from reactive recovery to proactive resilience, ensuring business continuity, operational certainty, and sustained performance in an increasingly unpredictable digital landscape.

Sources:

1.The Strategic Future of Subsea Cables - CSIS, 2025 | *2.Baltic cables damaged, Defense News, 2025*
3.Deep sea sabotage, Politico,eu, 2025 | *4.Digital 'catastrophe', Gulf News, 2026*

izo™ Core Connectivity

For more information, visit us at www.tatacommunications.com

CONTACT