India's connectivity risks: Subsea cables and satcom gaps

As geopolitical risks grow, India must strengthen communications resilience by turning satellite connectivity from a policy ambition into a dependable backup layer.

BY TONY VERGHESE & RADHIKA GUPTA

Most of the internet does not travel through space but runs under the sea. More than 95% of international data traffic is carried through submarine fibre-optic cables that support banking, cloud services, markets, and government communications.

This largely invisible infrastructure forms the backbone of the global digital economy and is increasingly exposed in a more contested geopolitical environment. India is deeply tied to cables landing along corridors to Europe, the Middle East, and Southeast Asia, making resilience planning an urgent strategic priority.

VULNERABILITY OF SUBMARINE INFRASTRUCTURE

Submarine cables are exposed in ways that terrestrial networks are not. Accidental damage, typically from ship anchors and fishing activity, remains common. Massive data flows traverse limited routes, and many of them traverse geopolitically sensitive waters.

Recent incidents in the Baltic and Red Seas have exposed the vulnerability of communications infrastructure and prompted renewed scrutiny of resilience planning. As geopolitical tensions intensify and conflicts become increasingly unpredictable,

> The greatest weakness in India's digital economy may lie far beyond its shores, where a few undersea routes carry traffic that keeps services moving for all users.

IN BRIEF

- Over 95% of international data traffic relies on submarine cables, making their security central to economic stability and national preparedness.
- Cable disruptions can affect payments, cloud services, markets and government networks, with remote and island regions facing greater risks.
- LEO satellites offer an alternative communications path, but regulatory, licensing and infrastructure hurdles limit readiness today.
- Security safeguards are essential, yet implementation delays can slow the deployment of redundancy designed to protect critical services.
- Satcom cannot replace fibre at the national scale, making clear emergency prioritisation frameworks vital during major disruptions.
- Faster spectrum decisions, gateway approvals and crisis protocols would strengthen India's communications resilience architecture.

chokepoints like the Strait of Hormuz add strategic risk to infrastructure once treated as purely commercial.

For India, a major cable cut would do far more than slow browsing. Overloaded alternate routes could raise latency across financial rails, disrupt payments and exchange operations, and impair emergency communications. Remote regions, island territories, and border areas, already sparsely connected, are especially exposed.

SATCOM: THE PROMISE VS. REALITY

Low-Earth-Orbit (LEO) satellite constellations can provide a geographically independent communications layer that is independent of subsea cable disruptions and can be deployed without laying fibre. In principle, satcom can cushion shocks by providing prioritised links for public safety, financial market utilities, and critical government users.

In practice, however, this redundancy remains largely unrealised because India's satcom ecosystem is still being operationalised.

POLICY DELAYS VS. OPERATIONAL READINESS

The Telecommunications Act, 2023, squarely brings satellite networks within the definition of telecommunication networks and shifts India to an authorisation-based framework. However, several key implementation issues remain unresolved.

The 'authorisation' framework under the Telecommunications Act, 2023, remains under active consideration, particularly on spectrum assignment methods, pricing, and coexistence conditions with terrestrial services.

Under the Unified License–Global Mobile Personal Communication by Satellite (GMPCS) framework, operators must meet stringent security conditions, including routing through Indian gateways and enabling lawful interception and monitoring.

Additional requirements, such as preventing location spoofing, mandating the use of domestic

> Satellite networks promise an independent communications layer, yet policy, licensing and operational barriers continue to delay credible readiness at scale today.

navigation systems like NavIC, and ensuring continuous authentication of user terminals, add operational complexity, particularly given the borderless nature of satellite coverage.

Delays in operationalising right-of-way rules across central, state, and local bodies continue to slow gateway deployment and the scaling of supporting fibre backhaul infrastructure.

These conditions are legitimate from a national security and sovereignty perspective. However, they also increase the time, cost, and complexity required to achieve operational readiness.

Satcom in India involves broadly three bodies: the Department of Telecommunications (licensing and spectrum), the Telecom Regulatory Authority of India (recommendations), and the Department of Space/ IN-SPACe (space ecosystem). While each institution plays an important role, overlapping responsibilities and sequencing challenges can delay implementation.

WHY SATCOM CANNOT REPLACE FIBRE

Even if fully operational, satcom is not a complete substitute for terrestrial or submarine infrastructure. A major terrestrial outage could generate traffic volumes that current satellite constellations are not designed to absorb at a national scale.

Even with improved LEO latency, aggregate throughput remains limited relative to the demands of hundreds of millions of users. Terminal costs, weather variability, and indigenous gateway requirements further constrain rapid scaling.

Resilience plans should clearly define emergency quality of service: who gets priority, the minimum uptime during congestion, and how nonessential traffic will be throttled.

To date, regulatory discussions have focused primarily on market access and spectrum pricing. By contrast, preparedness standards for large-scale disruptions arising from geopolitical events or infrastructure failures remain comparatively underdeveloped.

BALANCING SECURITY AND PREPAREDNESS

Security-driven safeguards, domestic gateways, interception readiness, and governance controls are justified. However, if approval processes, compliance integrations, and audit mechanisms are not calibrated to operational timelines, the redundancy they are intended to support may not be available when it is most needed. The policy question is no longer whether satcom matters, but whether India can operationalise it before a crisis forces it to rely on it.

A pragmatic path forward would include: publishing the satellite spectrum assignment framework with clear, time-bound milestones; adopting emergency waivers that pre-authorise limited relaxation of specified license conditions during declared crises, with audit safeguards; pre-clearing mission-critical user segments and quality of service tiers; and standardising gateway and interception compliance through test plans and certification.

These steps would allow operators to scale without prolonged, case-by-case approvals.

Caution in regulating satellite communications is both necessary and understandable. However, it must be accompanied by preparedness. Publishing the spectrum framework, codifying emergency response protocols, and streamlining security compliance mechanisms would help transform satcom from a policy inspiration into a credible layer of operational redundancy for India's critical communications infrastructure.

As India's digital economy continues to expand, resilience cannot be viewed solely as a technical consideration. It is increasingly a matter of economic scrutiny and national preparedness.

Verghese (left) and Gupta (right) are partners at JSA Advocates & Solicitors.
feedbackvnd@cybermedia.co.in