



KAMARAJ IAS ACADEMY
Only IAS Academy by Grandson of "Perunthalaivar Kamarajar"

India Ranks Among Top 10 Globally in Internet Blackout Preparedness, Yet Submarine Cable Dependence Remains a Key Vulnerability

Published On: 16-07-2026

Recent Developments:

- **India** ranked **9th globally** among nearly **100 countries** in preparedness to withstand a major **internet disruption**, according to a study by **TRG Datacenters**, a United States-based digital infrastructure provider.
- **The United States** secured the **1st position** with a vulnerability score of **0**, followed by **Indonesia** and the **United Kingdom**.
- India obtained a **vulnerability score of 23.4**, reflecting comparatively strong **digital resilience**, although dependence on a limited number of international submarine cable routes remains a significant concern.
- The ranking highlights the growing strategic importance of **digital infrastructure resilience**, **cybersecurity**, and **network redundancy** in ensuring uninterrupted digital connectivity.

India's Performance in Internet Blackout Preparedness:

Overall Ranking and Vulnerability Score:

- India ranked **9th** globally for its ability to withstand a large-scale internet disruption.
- The study uses a **vulnerability score**, where a **lower score indicates stronger resilience** against digital infrastructure failures.

Submarine Cable Connectivity:

- India is connected to the global internet through **22 submarine fibre-optic cable systems**, the lowest among the top ten ranked countries.
- In comparison:
 - **United States** – **115** submarine cables.
 - **Indonesia** – **72** submarine cables.
 - **United Kingdom** – **65** submarine cables.
- A relatively lower number of international cable routes reduces **route diversity** and increases dependence on common infrastructure.

Internet Exchange Points:

- India has **40 Internet Exchange Points (IXPs)** that enable domestic internet service providers and networks to exchange traffic directly.
- Internet Exchange Points:
 - Improve **internet speed** by reducing routing distance.
 - Lower network costs.
 - Reduce dependence on foreign transit networks.
 - Maintain domestic connectivity during international cable disruptions.

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477 / Whatsapp : 09710729833**

Electricity Infrastructure:

- Around **99.5%** of India's population has access to electricity.
- Reliable electricity supports uninterrupted functioning of:
- **Data centres.**
- **Cable Landing Stations.**
- **Telecommunication networks.**
- **Internet Exchange Points.**

Cybersecurity Preparedness:

- India received a **cybersecurity readiness score of 98.5 out of 100**, indicating strong capability to protect critical digital infrastructure against cyber threats and network disruptions.
- Strong cybersecurity reduces the likelihood of disruptions arising from malicious attacks.

Internet Usage:

- Approximately **70%** of India's population uses the internet.
- High internet penetration increases the economic, governance, and social consequences of prolonged internet disruptions.

Strengths and Vulnerabilities of India's Digital Infrastructure:

Major Strengths:

- India's resilience is supported by:
- A wide network of **Internet Exchange Points.**
- Near-universal electricity availability.
- High cybersecurity preparedness.
- Rapid expansion of domestic **data centre** infrastructure. India's operational data centre capacity has increased from **375 MW in 2020** to over **1500 MW by 2025**, with further growth expected.

Key Vulnerabilities:

- Limited **submarine cable diversity** creates dependence on a small number of international routes.
- Multiple telecom operators may rely upon:
- Common submarine cables.
- Shared cable landing stations.
- Common power infrastructure.
- Shared terrestrial fibre routes.
- Such shared infrastructure creates **single points of failure**, increasing systemic risk during disruptions.

Evidence Highlighting India's Exposure:

Red Sea Submarine Cable Incident:

- During **September 2025**, damage to submarine cables near **Saudi Arabia** slowed internet services across **India, Pakistan, and the United Arab Emirates.**
- The incident demonstrated that disruptions occurring outside India's territorial waters can still affect domestic digital connectivity.
- Although complete outages were avoided through traffic rerouting, users experienced increased latency and slower internet speeds.

Internet Blackout:

Meaning:

- An **internet blackout** refers to the complete or partial loss of internet connectivity across a locality, region, or country.
- It may affect international connectivity, domestic networks, or both, depending on the nature of the disruption.

Major Causes:

- Damage to **submarine fibre-optic cables**.
- **Cyberattacks** targeting critical digital infrastructure.
- Large-scale **power failures**.
- Hardware or software failures.
- **Natural disasters** such as earthquakes and tsunamis.
- Deliberate sabotage or armed conflict.
- Human activities such as ship anchors and fishing operations damaging submarine cables.

Components of Internet Infrastructure:

Submarine Fibre-Optic Cables:

- More than **99% of international internet data traffic** is carried through **submarine telecommunication cables**, making them the backbone of the global digital economy.
- These cables connect continents and support:
 - International communication.
 - Banking and financial transactions.
 - Cloud computing.
 - Digital commerce.
 - Government services.

Cable Landing Stations:

- Cable Landing Stations are facilities where submarine cables connect with terrestrial communication networks.
- They distribute international internet traffic into domestic fibre networks.

Internet Exchange Points:

- Internet Exchange Points allow internet service providers to exchange domestic traffic locally instead of routing it through foreign networks.
- Strong domestic exchange infrastructure improves network resilience during international disruptions.

Data Centres:

- Data centres store, process, and distribute digital information.
- A geographically distributed network of data centres reduces dependence on distant facilities and strengthens disaster recovery capabilities.

Traffic Rerouting During Cable Failures:

How Rerouting Works:

Kamaraj IAS Academy

Plot A P.127, AF block, 6 th street, 11th Main Rd, Shanthi Colony, Anna Nagar, Chennai, Tamil Nadu 600040

Phone: **044 4353 9988 / 98403 94477** / Whatsapp : **09710729833**

- When one submarine cable fails, internet traffic is redirected through:
- Alternative submarine cables.
- Different cable landing stations.
- Other Internet Exchange Points.
- Backup terrestrial fibre networks.
- Traffic rerouting usually prevents complete internet outages but may lead to:
- Higher latency.
- Reduced internet speed.
- Network congestion.

Impact of a Major Internet Blackout:

Economic Impact:

- Disruption of:
- Digital payments.
- Banking services.
- Stock markets.
- E-commerce.
- Cloud-based businesses.

Governance Impact:

- Interruptions in:
- Digital governance platforms.
- Public service delivery.
- Emergency response systems.
- Law enforcement communication.

Social Impact:

- Reduced access to:
- Online education.
- Telemedicine.
- Social communication.
- Remote working platforms.

Measures to Strengthen India's Digital Resilience:

Infrastructure Measures:

- Diversify international **submarine cable routes**.
- Establish additional **Cable Landing Stations** across different coastal locations.
- Expand domestic **optical fibre networks**.
- Promote geographically distributed **Internet Exchange Points**.
- Increase regional **data centre** capacity.

Operational Measures:

- Develop robust **disaster recovery mechanisms**.
- Conduct regular **network failover testing**.
- Ensure genuine **route diversity** across telecom operators.
- Strengthen protection of critical digital infrastructure through continuous cybersecurity monitoring.

Policy Measures:

- Promote public-private investment in resilient digital infrastructure.
- Enhance international cooperation for protection and rapid repair of submarine cable systems.
- Integrate digital infrastructure resilience into national **critical infrastructure protection** strategies. Recent international recommendations also emphasize coordinated action to improve submarine cable resilience and protect essential digital services.

Relevance for India:

Strategic Importance:

- India's expanding **Digital Public Infrastructure**, growing **digital economy**, increasing cloud adoption, and expanding **artificial intelligence** ecosystem require highly resilient communication infrastructure.
- Reliable internet connectivity is increasingly essential for **economic growth, national security, financial stability**, and **digital governance**.

Value Addition for UPSC:

Important Terms:

- **Internet Blackout.**
- **Digital Resilience.**
- **Submarine Fibre-Optic Cable.**
- **Cable Landing Station.**
- **Internet Exchange Point (IXP).**
- **Route Diversity.**
- **Network Redundancy.**
- **Critical Information Infrastructure.**
- **Disaster Recovery.**
- **Failover Mechanism.**

Important Institutions and Initiatives:

- **Indian Computer Emergency Response Team (CERT-In)** is the national agency for responding to cybersecurity incidents.
- **National Critical Information Infrastructure Protection Centre (NCIIPC)** protects critical information infrastructure under the **Information Technology Act, 2000**.
- **BharatNet** aims to expand high-speed broadband connectivity to rural India.
- **Digital India Programme** seeks to strengthen digital infrastructure as a core utility for governance and public service delivery