International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 1-7

Influence of American - Iran conflict on Internet based services in Asian Countries: Special Reference to India and China

Dr M Raghavendra[1]
Librarian (SG)
Government First Grade College (Autonomous), Gubbi - 577216
Email: raghushira@gmail.com

Manjula V[2]
Research Scholar
Department of Library and Information Science
Mohan Babu University, Tirupati, Andhra Pradesh
Email: monimanju@gmail.com

Abstract: The global Internet infrastructure is critically dependent on submarine fiber optic cable systems that traverse the deep ocean, carrying over 97% of international data traffic. Geopolitical tensions, particularly conflicts involving major powers such as the United States and Iran, have direct and indirect consequences on these under sea communication systems. This paper analyzes the impact of such conflicts on Internet based services in Asian countries, with special reference to India and China. It also presents a detailed technical examination of submarine cable structure, deep-sea deployment, and interconnection networks among nations.

Keywords: Submarine Cables, Internet Infrastructure, Geopolitics, US–Iran Conflict, India, China, Fiber Optics, Deep Ocean Communication

I. Introduction

The rapid expansion of Internet-based services has transformed the global economy, enabling seamless communication, digital trade, cloud computing, and real-time data exchange across nations. Despite its seemingly wireless nature, the Internet fundamentally depends on a vast network of submarine fiber-optic cables laid across the ocean floor, which carry nearly 95–99% of international data traffic. These undersea cables form the backbone of global connectivity, linking continents and supporting critical sectors such as banking, governance, education, and e-commerce.

In recent years, geopolitical tensions have increasingly intersected with digital infrastructure, bringing attention to the vulnerability of submarine cable networks. The ongoing conflict involving the United States and Iran has emerged as a significant concern in this context, particularly due to its proximity to strategic maritime chokepoints such as the Strait of Hormuz and the Red Sea. These regions host a dense concentration of submarine cables that connect Asia with Europe and Africa, making them crucial nodes in global Internet architecture.

The escalation of conflict in these areas has raised fears of potential disruptions to Internet infrastructure, either through direct damage, restricted access for maintenance, or strategic threats. Reports indicate that even the possibility of interference with undersea cables in these regions can significantly impact global connectivity, leading to increased latency, reduced bandwidth, and interruptions in digital services. Furthermore, recent developments suggest that ongoing tensions have already delayed major submarine cable projects and affected existing routes linking multiple Asian countries.

Asian nations, particularly India and China, are highly dependent on these submarine networks for their economic and technological activities. For instance, a substantial portion of India's Internet traffic especially connections to Europe passes through cable systems located in geopolitically sensitive regions such as the Gulf and Red Sea. Similarly, China's growing digital economy and its strategic investments in global communication infrastructure make it equally sensitive to disruptions in undersea connectivity.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 1-7

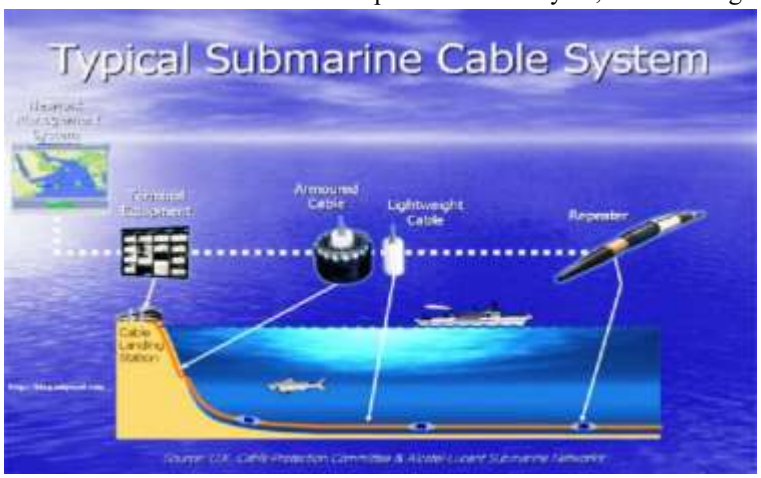
Against this backdrop, the American–Iran conflict represents not only a military or political confrontation but also a potential threat to global digital infrastructure. The implications extend beyond regional instability, affecting Internet performance, data security, and economic continuity across Asia. This study aims to analyze the influence of the American–Iran conflict on Internet-based services in Asian countries, with special reference to India and China, while also examining the structural and strategic importance of deep-sea submarine cable systems and their interconnections among nations.

II. Structure and Design of Submarine Internet Cables

Submarine Internet cables form the physical backbone of global digital communication, carrying the vast majority of international data traffic across oceans. Their structure and design are highly sophisticated, engineered to ensure durability, efficiency, and long-term reliability under extreme deep-sea conditions.

2.1 Basic Structure of Submarine Cables

submarine cable consists of multiple concentric layers, each serving a specific function



Optical Fiber Core: The innermost component contains thin strands of glass fibers that transmit data in the form of light pulses. These fibers are capable of carrying terabits of data per second over long distances.

Gel or Waterproof Coating: Surrounding the fibers is a gel-like substance that protects against water ingress and cushions the fibers from mechanical stress.

Copper or Aluminum Tube: This metallic layer conducts electrical power required to operate repeaters (signal amplifiers) placed along the cable.

Steel Wire Armoring: High-tensile steel wires provide strength and protection, especially in shallow waters where cables are exposed to human activities like fishing and anchoring.

Polyethylene Outer Jacket: The outermost insulating layer protects the cable from corrosion, abrasion, and environmental damage.

2.2 Signal Transmission and Repeaters

Data is transmitted through optical fibers using light signals generated by lasers. As signals travel long distances, they weaken due to attenuation. To address this, optical repeaters (amplifiers) are installed at intervals of approximately 50–100 km along the cable. These repeaters boost the signal without converting it back to electrical form, ensuring high-speed and efficient communication across continents.

2.3 Cable Types Based on Depth

Submarine cables are designed differently depending on the depth of the ocean:

- Deep-Sea Cables: These are relatively thinner and lighter, as they rest undisturbed on the ocean floor at depths exceeding 2000 meters.

- Shallow-Water Cables: These have additional armoring layers to protect against external threats such as ship anchors, trawling nets, and coastal activities.
- Buried Cables: In coastal regions, cables are often buried 1–2 meters beneath the seabed using specialized ploughing machines to prevent damage.

2.4 Cable Landing Stations and Interconnections

Submarine cables connect to terrestrial networks through landing stations, which are critical infrastructure points located along coastlines. These stations convert optical signals into electrical signals for land-based networks, route data to Internet service providers (ISPs) and data centers, act as interconnection hubs linking multiple countries, countries like India and China have several strategic landing stations (e.g., Mumbai, Chennai, Shanghai), making them key nodes in global Internet connectivity.

2.5 Design Considerations and Challenges

The design of submarine cables must address several engineering and environmental challenges,

- High Pressure: Deep ocean pressures can exceed 8000 psi
- Corrosion Resistance: Materials must withstand saltwater exposure for decades
- Seismic Activity: Earthquakes and underwater landslides can damage cables
- Human Interference: Fishing, anchoring, and maritime traffic pose risks

To mitigate these challenges, modern cables incorporate advanced materials, real-time monitoring systems, and redundant routing strategies.

2.6 Lifespan and Maintenance

Submarine cables typically have a lifespan of 20–25 years. Maintenance is carried out using specialized cable repair ships that locate faults, retrieve damaged sections, and restore connectivity. Due to their critical role, even minor disruptions can have significant global impacts.

III. Internet or ICT Based Services in Asian Countries

In the contemporary digital era, internet based services have become an essential part of economic, social, and technological development across Asian countries. From online banking and e-commerce to cloud computing and digital governance, these services rely heavily on robust communication infrastructure. At the core of this infrastructure lies a vast network of submarine (under sea) fiber optic cables, which serve as the backbone of global internet connectivity. Asia, being one of the most dynamic and densely populated regions, depends significantly on these cables for high-speed and reliable data transmission.

Internet-based services refer to all services that operate through the internet. These include:

- E-commerce platforms
- Online education systems
- Digital banking and financial services
- Cloud computing and data storage

- Social media and communication services
- E-governance and public service delivery

Countries like India, China, Japan, and Singapore have witnessed rapid expansion in these services due to increased internet penetration and technological advancement. Asia is interconnected through an extensive network of submarine cables linking major coastal cities and countries. Important routes include:

- India to Europe via the Middle East
- China and Japan to North America via the Pacific Ocean
- Southeast Asia connecting to Australia and other Asian regions

Major landing stations are located in cities such as Mumbai, Chennai, Singapore, Shanghai, and Tokyo. These stations act as gateways that connect international cable networks with domestic internet infrastructure. This interconnected network ensures seamless data transmission across borders, supporting international trade, communication, and technological collaboration.

Submarine internet cables are the invisible yet indispensable infrastructure supporting internet-based services in Asian countries. They enable high-speed, reliable, and large-scale data transmission across continents, fostering economic development, technological progress, and global integration. As Asia continues to advance digitally, the importance of secure, efficient, and well-maintained submarine cable networks will only increase. Ensuring their protection and expansion is vital for sustaining the region's digital future.

3.1. Role in Supporting Internet Based Services

Submarine cables play a crucial role in enabling various internet-based services in Asia:

- **Economic Growth**: They facilitate global trade, outsourcing, and digital economies.
- **Communication**: Support real-time communication through emails, messaging apps, and video conferencing.
- **Education and Research**: Enable online learning platforms and academic collaborations.
- **Financial Systems**: Ensure secure and fast digital transactions across borders.
- **Entertainment**: Support streaming services and online gaming industries.

Countries like India and China rely heavily on these cables to support their growing digital populations and expanding IT sectors.

Major internet hubs in Asia are the pillars of the region's digital infrastructure. Cities like Singapore, Mumbai, Chennai, Shanghai, Hong Kong, and Tokyo act as critical nodes that connect Asia to the global network. They support economic growth, technological advancement, and seamless communication across borders. As the demand for internet-based services continues to rise, the role of these hubs will become even more significant in shaping Asia's digital future.

IV. Impact of war on internet services on asian countries

Armed conflicts can have a serious impact on submarine (undersea) internet cables, which are the backbone of connectivity for Asian countries. In situations such as tensions involving the Red Sea or the Persian Gulf, physical damage to cables whether accidental or deliberate can disrupt major data routes linking Asia with Europe and other regions. Since a significant portion of Asia's international internet traffic passes through these strategic corridors, any cable cut can lead to slower internet speeds, service outages, and increased latency across countries like India, China, and Southeast Asian nations. Such disruptions can affect critical sectors including banking, e-commerce, cloud services, and communication systems, leading to economic losses and reduced efficiency. Moreover, wars may delay repair operations due to security risks, prolonging outages and forcing data rerouting through longer paths, which further strains network capacity. Thus, conflicts in key maritime regions pose a direct threat to the stability and reliability of internet-based services in Asia.

4.1 Precautions to Control the Impact of war on ICT services in Asia

Conflicts in strategically sensitive regions such as the Red Sea, South China Sea, and Persian Gulf can disrupt Information and Communication Technology (ICT) services by damaging submarine cables, data centers, and communication infrastructure. To minimize such impacts, Asian countries must adopt a combination of technical, strategic, and policy level precautions.

4.2 Diversification of Network Routes
Countries should avoid dependence on a single cable route by developing multiple submarine cable connections through different geographical paths. This ensures that if one route is disrupted due to conflict, alternative paths can maintain connectivity.

4.3 Development of Redundant Infrastructure
Redundancy is essential for resilience. Establishing backup systems such as, Additional submarine cables, Satellite communication links, and terrestrial cross-border fiber networks can help maintain continuity of ICT services during disruptions.

4.4 Strengthening Regional Cooperation
Asian countries should collaborate through regional organizations and agreements to share infrastructure, provide mutual support during outages, develop joint strategies for protecting communication networks, such cooperation enhances collective security and reduces vulnerability.

4.5 Protection of Critical Infrastructure
Governments must identify submarine cables and ICT systems as critical infrastructure and ensure their protection by monitoring sensitive maritime zones, deploying naval surveillance around cable routes, implementing strict security protocols at landing stations.
The impact of war on ICT services in Asian countries can be severe, but it can be effectively managed through proactive planning and strategic investment. By diversifying networks, strengthening infrastructure, enhancing regional cooperation, and adopting advanced technologies, countries can ensure the resilience and stability of their ICT systems even in times of conflict.

V. Precautions needs to be taken

Controlling wars and minimizing their impact on critical infrastructure especially network stations and communication systems requires a combination of diplomatic, strategic, and technological measures. International efforts through organizations like the United Nations play a vital role in conflict prevention, peacekeeping, and promoting dialogue between nations to avoid escalation. Establishing international agreements to recognize telecom infrastructure as protected civilian assets similar to conventions governing war conduct can reduce deliberate targeting of network stations. At the national level, governments should strengthen infrastructure resilience by decentralizing network stations, building redundant systems, and securing key facilities against both physical and cyber threats. Advanced monitoring technologies, early warning systems, and rapid-response repair teams can help limit damage and restore services quickly if disruptions occur. Additionally, fostering regional cooperation among countries ensures shared responsibility in protecting communication networks and maintaining connectivity during crises. Together, these measures help reduce both the occurrence of conflicts and their damaging effects on vital digital infrastructure.

VI. Global policy measures for safety

In the modern digital era, communication infrastructure such as network stations, data centers, and submarine cable landing points forms the backbone of global connectivity. However, wars and geopolitical conflicts pose a serious threat to these critical systems, leading to large-scale disruptions in communication, economic activities, and governance. Network stations, which act as central nodes for data transmission, are particularly vulnerable during conflicts. Therefore, it is essential to formulate effective policies to control wars and minimize their impact on such vital infrastructure.

6.1 Need for Policy Intervention
The increasing dependence on Information and Communication Technology (ICT) has made infrastructure protection a priority for nations. Damage to network stations can lead to:

- Breakdown of communication systems
- Disruption of financial and digital services
- Loss of critical data and national security risks
- Economic instability and social disruption

Thus, proactive policy measures are necessary not only to prevent conflicts but also to safeguard infrastructure during crises.

6.2 International Policies and Agreements

Global cooperation plays a crucial role in controlling wars and protecting infrastructure. Organizations such as the United Nations can facilitate peacekeeping and conflict resolution through diplomatic channels.

Recognition of ICT Infrastructure as Protected assets international laws should classify network stations and communication systems as civilian infrastructure that must not be targeted during conflicts. Strengthening International Humanitarian Law expanding frameworks similar to the Geneva Conventions to include digital and communication infrastructure can help reduce intentional damage. Multilateral Agreements countries should enter agreements to jointly protect submarine cables and network facilities, ensuring uninterrupted global connectivity.

6.3 National-Level Policy Measures

Governments must implement strong domestic policies to protect network stations:

- Infrastructure Security Planning: Establish secure locations for network stations with physical protection systems, surveillance, and restricted access.
- Decentralization of Network Systems: Avoid concentration of critical infrastructure in a single location by distributing network stations across multiple regions.
- Redundancy and Backup Systems: Develop alternative communication channels such as satellite links and backup servers to ensure continuity during disruptions.
- Emergency Response Frameworks: Create rapid response teams for quick repair and restoration of damaged infrastructure.

6.4 Technological Policies for Resilience

Technology can significantly reduce the impact of war on infrastructure:

- Cyber security Measures: Implement strong encryption, firewalls, and intrusion detection systems to protect against cyber attacks.
- Use of Artificial Intelligence: AI-based monitoring systems can detect threats and predict potential failures in network infrastructure.
- Cloud and Distributed Systems: Storing data across multiple locations reduces the risk of complete data loss.

6.5 Regional Cooperation in Asia

Asian countries must collaborate to protect shared infrastructure such as submarine cables and cross-border networks. Regional cooperation can include:

- Joint monitoring of cable routes
- Sharing technical expertise and resources
- Coordinated response strategies during emergencies

Such collaboration enhances resilience and ensures continuity of services across nations.

6.6 Conflict Prevention Strategies

Preventing war is the most effective way to protect infrastructure. Policies should focus on:

- Diplomatic negotiations and peaceful dispute resolution
- Economic cooperation and interdependence
- Confidence-building measures among nations
- Promoting international peace initiatives

Reducing tensions directly reduces the risk of infrastructure damage.

6.7 Challenges in Policy Implementation

Despite the importance of these policies, several challenges exist:

- Lack of global consensus on infrastructure protection
- Political and strategic conflicts among nations
- High costs of infrastructure development and security
- Rapidly evolving cyber threats

Addressing these challenges requires continuous international dialogue and investment. The protection of network stations and communication infrastructure during times of war is essential for maintaining global connectivity and economic stability. Effective policies must combine international cooperation, national preparedness, and technological innovation. By recognizing ICT infrastructure as a critical and protected asset, strengthening legal frameworks, and promoting peace, nations can significantly reduce the impact of conflicts on digital systems. Ultimately, a balanced approach focusing on both conflict prevention and infrastructure resilience is key to ensuring sustainable development in the digital age.

VII. Conclusion

The influence of the American Iran conflict on internet based services in Asian countries, particularly India and China, highlights the critical dependence of modern digital systems on fragile geopolitical environments. The conflict has exposed the vulnerability of submarine cable networks passing through strategic choke points such as the Strait of Hormuz and the Red Sea, which carry a substantial portion of Asia's international data traffic. For instance, a significant share of India's internet connectivity to Europe relies on cables routed through these regions, making it highly susceptible to disruptions during conflict .

While countries like China may experience relatively moderated direct impacts due to diversified connectivity and strategic positioning, the broader Asian region faces risks such as increased latency, rerouting of data, service slowdowns, and economic losses. The conflict also demonstrates how modern warfare extends beyond physical battlefields into digital infrastructure, affecting cloud services, financial systems, and communication networks.

In conclusion, the American Iran conflict underscores the urgent need for resilient infrastructure, diversified cable routes, and strong international cooperation to safeguard internet based services. As Asia continues to advance digitally, ensuring the security and stability of undersea cable networks will remain essential for sustaining economic growth, technological development, and uninterrupted global connectivity.

The political science argument is strengthened by connecting governance, information access, user satisfaction and fuzzy cognitive modelling [6], [7], [5], [8]. This literature is relevant because public policy and digital governance increasingly require transparent, adaptive and citizen-oriented decision frameworks. Additional governance and AI-policy references are added for broader support [9]-[11].

References

[1] Starosielski, N, "The undersea network," Duke University Press, 2015.
[2] Burnett, D. R., Beckman, R., & Davenport, T. M. (Eds.), "Submarine cables: The handbook of law and policy," Martinus Nijhoff Publishers, 2014.
[3] International Telecommunication Union, "The state of broadband 2024: Leveraging AI for universal connectivity," ITU and UNESCO Broadband Commission, 2024.
[4] TeleGeography, "Submarine cable map," TeleGeography, 2024.
[5] Chetana, R., Yogeesh, N., Jabeen, F. T. Z., & Girija, D. K, "Exploring uncertain data with fuzzy logic in cultural heritage conservation," Library Progress International, 44(3), 14416-14424, 2024.
[6] Yogeesh, N., Chetana, R., Vasanthakumari, T. N., & Ramesha, M. S, "Fuzzy logic in knowledge management: A model for adaptive information access," Library Progress International, 44(3), 14433-14441, 2024.
[7] Girija, D. K., Yogeesh, N., & Rashmi, M, "Fuzzy cognitive maps for analyzing user satisfaction in information services," Library Progress International, 44(3), 14425-14432, 2024.
[8] N. Yogeesh, "Mathematics application on open source software," Journal of Advances and Scholarly Researches in Allied Education, vol. 15, no. 9, pp. 1004-1009, 2018.
[9] UNDP, Digital Strategy 2022-2025. New York: United Nations Development Programme, 2022.
[10] Government of India, Digital Personal Data Protection Act, 2023. New Delhi: Ministry of Law and Justice, 2023.
[11] OECD, Recommendation of the Council on Artificial Intelligence. Paris: OECD, 2019.