International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 06, June 2022)

An Analysis on Impact of Splinternet in India

Shriram Dhurwey[1], Sunil Kispotta[2], Swapnil Nagayach[3], Vedant Khare[4], Shravan Richhariya[5], Ishita Sharma[6]

[1]Assistant Professor, Department of Information Technology, JEC, Jabalpur (M.P.), India
[2]Assistant Professor, Department of Computer Science & Engineering, JEC, Jabalpur (M.P.), India
[3]UG Student, Department of Information Technology, JEC, Jabalpur (M.P.), India
[4,5,6]UG Student, Department of Electronics and Telecommunication, JEC, Jabalpur (M.P.), India

[1]srdhurve@jecjabalpur.ac.in, [2]skispotta@jecjabalpur.ac.in, [3]Swapnilnagayach2510@gmail.com,
[4]Vedantkhare123@gail.com, [5]Richhariyashra1@gmail.com, [6]*Ishi.sharma3009@gmail.com*

***Abstract:-* India is a developing country with limited global control, particularly in the field of cyberspace and the internet; while we have made significant progress, we continue to face cyberattacks and other difficulties. However, the domain of security threats has been greatly expanded by NATO's restrictions on Russia, which raises concerns about the Internet and threatens Indian Welfare Schemes and Development based on the Internet, such as DBT (Direct Bank Transfer) or Banking Mechanisms (NEFT), particularly at a time when we are reaching new milestones.**

As a result, this Research Paper attempted to present a Possible Step of the Internet, as well as suggestions on how we might achieve it, as well as advantages and disadvantages, as well as what steps have been taken in that direction, as well as a brief case study of China.

I. Introdution

The tremendous growth of the Internet over the last decade has sparked a parallel trend in nation governments' efforts to tailor the Internet to their populations' wants and expectations. The monopolistic dominance of a few large Internet corporations (Tech Gaints) has contributed to the establishment of cyberislands, which confine Internet users in closed eco-systems of services and content. The global Internet, which was once envisioned as being free and unfettered, is presently under severe strain and is likely to fracture into fragments of bounded networks.

Some countries have experimented with a national Internet model in which Internet services and content are distributed only within their borders, with no reliance on the global Internet (Russia,China). Others have used censorship, data localization, and data protection laws and directives to cut out sections of the Internet that they deem appropriate (India, European Union ,Uk etc.).

These Tendencies are expected to reach a new peak once NATO Forces (US and Allies) weaponize cyberspace and internet facilities in an attempt to dissuade Russia from using global connectivity via the Internet. The US-led bloc was able to pursue a number of tech companies, including Meta (Facebook, Instagram, Whatsapp, and others), Google, and others, in order to impose restrictions on Russians. They also pushed Russia out of the SWIFT banking system, distorting global trade and paralysing Russia's banking system. Many developing and developed countries throughout the world are concerned about NATO's actions, which has increased their demand for self-sufficient and long-term internet infrastructure and mechanisms (Splinternet)

The phenomena of splintering the Internet into several apparent Internet instances where the experience, services, and information available vary dramatically depending on a user's location is known as Internet fragmentation, resulting in TheSplinternet.

The constant targeting of India and its government by the western world, as well as the threats posed by China and Pakistan, pushes India to seek more Internet sovereignty and security, potentially paving the way for India's own Splinternet.

II. Need For Splinternet

The failure of like-minded countries to communicate a consistent and inclusive message about the value of internet freedom and openness for innovation and development has eroded public confidence.

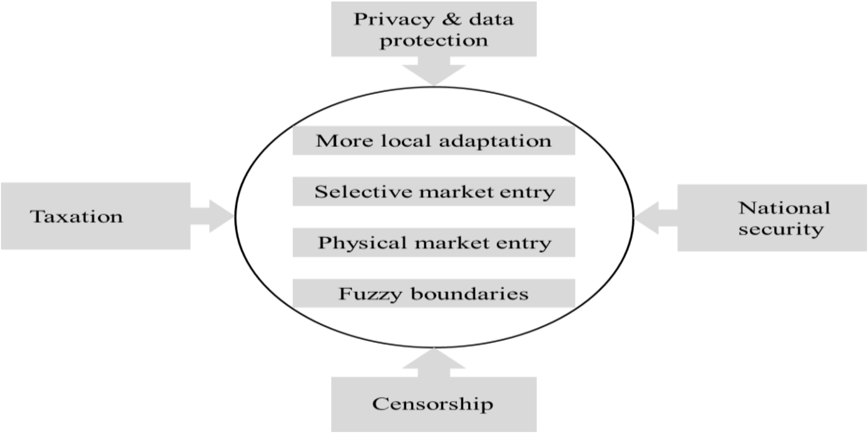
The Snowden revelations in 2013, followed by allegations of social media-based election meddling, have tempered early internet utopian visions.

The ethics of US platform business models have been called into question, and the US has lost moral credibility as the defender of a global, free, and open internet.

Through legislation like the General Data Protection Regulation (GDPR) and groundbreaking judicial decisions from the European Union's Court of Justice, Europe has established itself as the gold standard for privacy (EU).

Data leaks by numerous global techgaints, such as the Facebook analytica Scandal, Pegasus Spyware Scandal, and others, are also a problem.

Forces Driving Fragmentation and Implications



III. Measuring Fragmentation

The topic of Internet fragmentation encompasses politics, Internet governance, commercial goals, mechanisms, and technology. We're focusing on assessing the existing and prospective future influence on Internet architecture and operational functionality by monitoring the diversity of fragmentation types, methods, and frequency. Fragmentation examines side effects and wasteful applications of technology and, where suitable, proposes alternate solutions and remedies.

To capture the multifaceted character of fragmentation, measuring Internet fragmentation necessitates the integration of new and existing Internet measurement technologies. The most common reasons of fragmentation on the Internet include web and application blocking, Internet shutdowns, and packet filtering. These are necessary tools for any sovereign government to maintain law and order. The Indian Constitution permits the government to do so (Art 38, for example) but with reasonable restrictions. Even the Supreme Court of India, in its decision in the AnuradhaBhasin V/S Union Of India case, reaffirmed this.

There's also a growing list of intriguing data sources to comb through in order to account for as many different sorts of fragmentation as feasible. (1) data localization policies, (2) Freedom House's Freedom On The Net(FOTN) ranking, (3) Internet user population, and (4) National Chokepoint Potential(NCP), which determines the likelihood of fragmentation practises due to optimal filtering system positioning facilitated by AS topology arrangement in a country. In terms of these parameters, India performs well only in terms of Internet user population, which has recently improved too much after 2017 (Jio Movement), but in all other areas, India is ranked fairly low due to regular impositions of Sec 144 CrPC, UAPA, AFSPA, and other regulations. aggregated view of these data sources to observe fragmentation Current Internet measurement systems, such as (1)CensoredPlanet, (2)Internet Outage Detection and Analysis(IODA), (3)Open Observatory of Network Interference(OONI), (4)Access Now Shutdown Tracker Optimization Project(STOP), and others, were designed to track specific performance, censorship, and service availability observations. These systems do not have the depth or breadth to measure fragmentation holistically on their own.

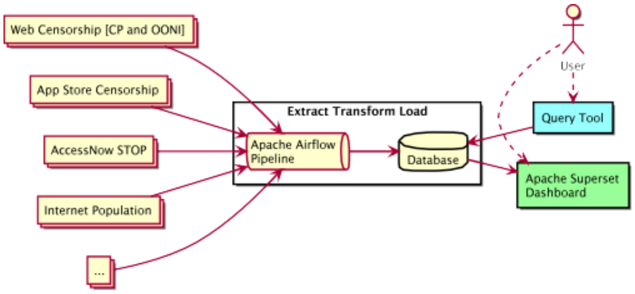


Figure 1: System high level design

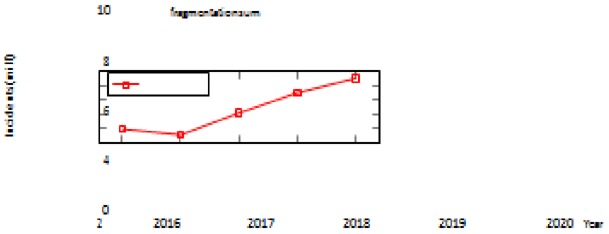


Figure 2: Global fragmentation trending plot

Reference: Splinternet: How geopolitics and commerce are fragmenting the World Wide Web

How India Can Create Its Splinternet ?

1) The installation of mandatory technical equipment to counter threats

For assurance and technical standardisation, produced in India equipment is most likely to be used.

2) In the event of a threat, centralised management of telecommunication networks and a control system for connecting lines crossing India's border

   a) Authorities enact new laws and policy measures, requiring ISPs to comply with them early on, and traffic is directed through "choke points," network nodes through which data passes when entering or exiting a country's internal network. Because of their belief in the Global Free Internet Concept and a lack of technological capacity, countries like the United Kingdom, India, and Russia currently have significantly less control over their networks and domestic ISPs.

   b) The ability to monitor traffic at the source, without the use of an ISP or internet services that do not adhere to current regulations.

      (a) The process of installing DPI systems or a similar technology

Inspection of the packet in detail

DPI (deep packet inspection) is a sophisticated method of inspecting and regulating network traffic. It's a type of packet filtering that finds, identifies, classifies, and reroutes or rejects packets with certain data or code payloads that traditional packet filtering, which simply looks at the headers, misses.

DPI systems' core technical components are so-called black boxes, which are put at internet provider hubs to examine both data packets and communication content. They allow for request monitoring, filtering, and slowing, as well as banning of certain content. Each data packet can also be assigned to a certain service or application by the black boxes.

Data packets, even those delivered through an encrypted connection, must always be sent to a specific destination and must have a visible address. This information cannot be encrypted because an ISP would otherwise be unable to determine to which address the user's request should be sent (d) Monitoring VPN services and their users (e) Technology that can be used and tackled efficiently Domain After the ban in Russia, Telegram employed fronting domain fronting, a technique in which a request is forwarded on the same server after an HTTPS connection has been established.

1. to the network's integrity, such as when no connection can be established between users; 2. to the network's stability, such as when equipment fails or is disabled due to natural or man-made disasters; 3. to the network's safety of operation, such as when hackers attack the network and ISPs are unable to defend against the attack, or when ISPs themselves cause disruption.

Solution: Pseudo decentralised internet infrastructure (PDII) is a network-centric internet that combines the data link and network layers. It reorganises the internet's architecture and redefines identifiers. It also represents a departure from the internet's long-standing 'best effort' approach, guaranteeing a guaranteed level of service and low latency instead.

Despite being touted as 'decentralising,' the technologies (for example, distributed ledger technology (DLT)) enable centralised control and command of the internet through fine-grained micromanagement and surveillance, which is likely backed by 5G's edge computing. Centralized control is made possible by merging the data connection and network layers.

It takes intelligence away from the internet stack's end nodes (i.e. application layer) and into the hands of network operators and infrastructure providers, who can then be managed centrally by the government.

However, while the internet's underlying architecture including the Transmission Control Protocol and Internet Protocol (TCP/IP) are being reinvented,

Lightweight, open, and interoperable technical standards must play a major role in keeping the internet together as a unified, global network that allows for technological innovation and economic progress. As a result, conventional 'end to end' principles with 'dumb pipes' (e.g. networks and routing) that handle data neutrally and allow innovation to happen at the network's edges are being replaced.

3) The establishment of a national domain name system for India (IDNS)

There has never been a country that has succeeded in creating a proprietary national DNS. As a result, it's difficult to say if such a system could coexist with the current global DNS, which is assigned and maintained by the International Corporation for Assigned Names and Numbers (ICANN). A national DNS would only make sense if a country chooses to isolate its internet for the long run.

This will isolate Indian websites from the global DNS, rendering them inaccessible in the rest of the world. India would most likely be unable to use the global DNS at the same time.

NEED: Because ICANN is a non-profit organisation, government involvement is virtually impossible. The US government, on the other hand, is most certainly technically and politically capable to shutting down domains associated to websites all over the world.

IANA (Internet Assigned Numbers Authority), a division of ICANN in California, is in charge of the global DNS. Top-level domains (TLDs) such as.ru and.de are stored in root zone files. These files, which are administered by ICANN and serve as the internet's backbone, are principally held on 13 root zone servers throughout the world, 10 of which are in the United States and one each in the Netherlands, Sweden, and Japan. TLD files, on the other hand, are stored on a variety of additional name servers.

If the ten root servers on US soil be adjusted to redirect website domains, for example, there are still three more root servers and all name servers in US-controlled countries.

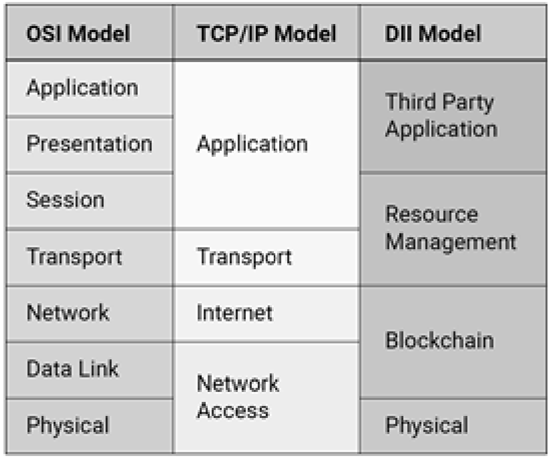
When root zone file manipulation is identified, DNS providers can halt the mirroring process from US root servers, but the situation can still be controlled.

4) The use of encrypted everything' protocols, especially in IETF (Internet Engineering Task Force) standards

5) Internet that is network-centric, combining internet layers, particularly the data link and network layers.

It reconceptualizes identifiers and restructures inter-net architecture. It also represents a departure from the internet's long-standing 'best effort' approach, guaranteeing a guaranteed level of service and low latency instead. Despite being touted as 'decentralising,' the technologies (for example, distributed ledger technology (DLT)) enable centralised control and command of the internet through fine-grained micromanagement and surveillance, which is likely backed by 5G's edge computing.

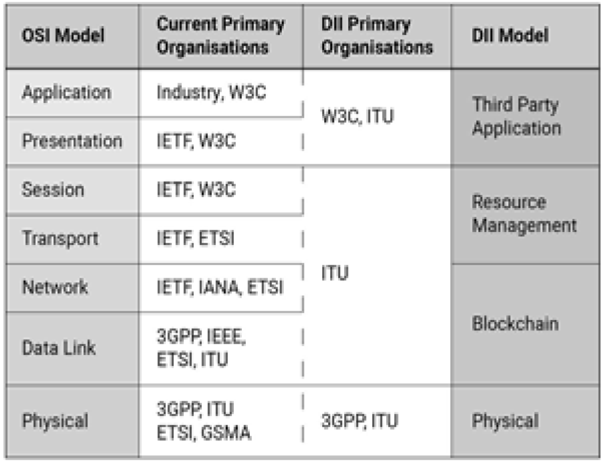
Centralized control is made possible by merging the data connection and network layers. It pushes intelligence away from the internet stack's end nodes (i.e. application layer) and into the hands of network operators and infrastructure providers, which may then be exploited centrally by the government.



OSI Model	TCP/IP Model	DII Model
Application	Application	Third Party Application
Presentation		
Session		Resource Management
Transport	Transport	
Network	Internet	Blockchain
Data Link	Network Access	
Physical		Physical

Figure 1.Comparison of internet layer models.

6) Increasing Presence In Global Networking Management Institutions



OSI Model	Current Primary Organisations	DII Primary Organisations	DII Model
Application	Industry, W3C	W3C, ITU	Third Party Application
Presentation	IETF, W3C		
Session	IETF, W3C	ITU	Resource Management
Transport	IETF, ETSI		
Network	IETF, IANA, ETSI		Blockchain
Data Link	3GPP, IEEE, ETSI, ITU		
Physical	3GPP, ITU ETSI, GSMA	3GPP, ITU	Physical

7) Creating a new Identifier Repository using the name TCP/IP protocols, which underpin the internet, include Alternative Identifiers as a major component. Any solution that aims to replace TCP/IP must provide a system of unique identifiers in order to achieve acceptance.

Splinternet's Benefits:

1) Secure and Self-Governed Cyberspace
2) Self-Sustained System of Connectivity in the Event of Global Connectivity Failure/Rupture
3) Protection against external threats and state-sponsored assailants

Possible Splinternet Threats

1. It has the potential to become a government kill switch, allowing governments to infringe on people's rights to freedom (Art 19 to 22)

It can be used to disable much of India's internet. Even DPI bypass systems, VPNs, and other unnamed connections will not work in the case of a shutdown — communication becomes physically impossible.

2. Can Result In A Privacy Breach
3. Excessive power Threat to Democratic Values in the Hands of Executives (Breach of Privilege)
4. encrypted everything' protocols, especially those found in IETF standards. Implementations of DNS over HTTPS (DoH), for example, encrypt sensitive data in transit but could rearrange domain name resolution both technically and administratively. For governments, such technologies are both a menace and an opportunity.

India's Current Situation

The Indian government has taken a few recent steps that indicate a desire to exert greater control over the Internet, whether in terms of data, security, or other dimensions.

A few recent examples are:

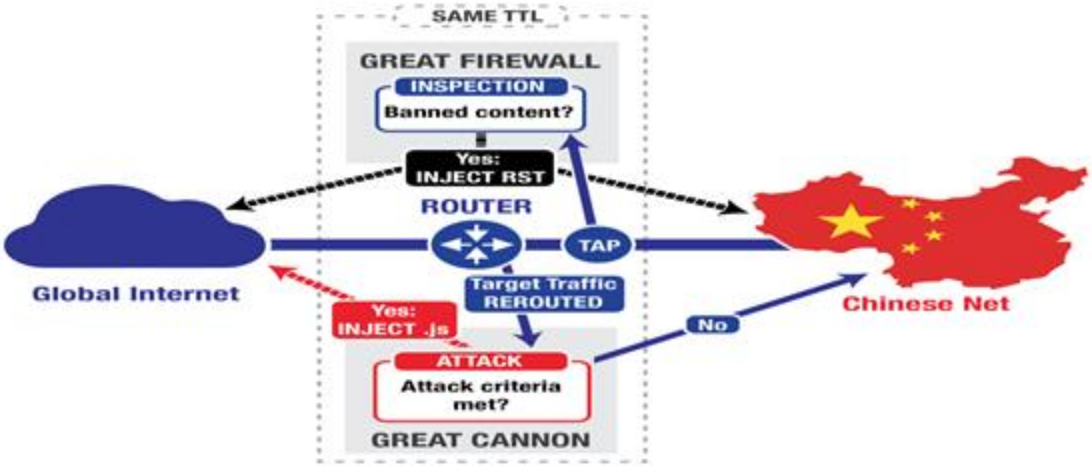
1. Chinese Apps are Banned (June 2020)
2. Conditions for Data Localization for Tech Gaints (2018)
3. Requesting that VPN service providers produce reports on their users, etc (2022)

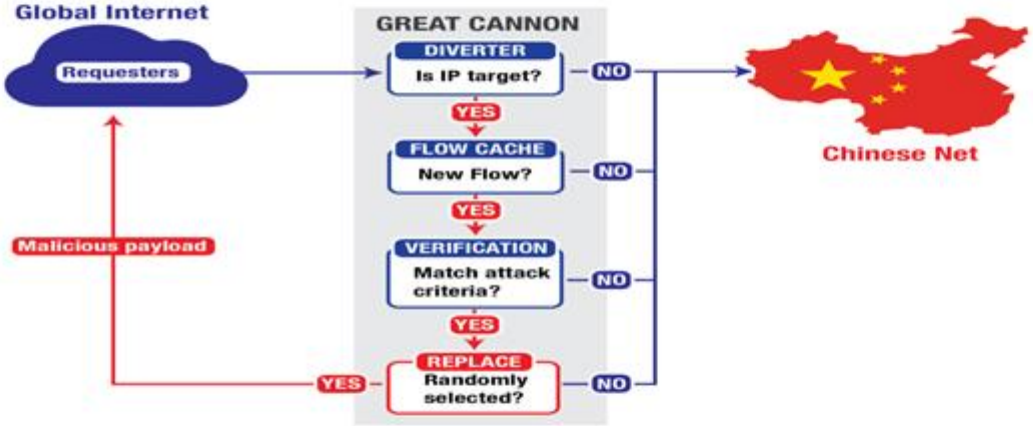
China: A Brief Case Study

I've devised a two-pronged strategy.

2 The Great Cannon 1 The Great Wall (firewall) (Cyber attack Mechanism)

China is likewise attempting to establish its own Splinternet, and discussions on Internet Protocols and Processes began in 2018.





IV. Conclusion

Splinternet may be a near-term possibility in the future, alongside the Global Internet; recent government actions around the world, notably India, suggest similar inclinations.

Such active enthusiasm for self-sufficiency and sustainability in the shape of Splinternet requires a heavy reliance on Internet-based services and governance models.

(*To Avoid:* Internet Rupture -> Governance Rupture Scenarios)

REFERENCES

[1] Standardizing the splinternet: How Chinese technical standards may fragment the internet https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1805482

[2] Understanding Russia's "Sovereign Internet Law": Improving Control and Speeding Up the Splinternet https://www.ssoar.info/ssoar/bitstream/handle/document/66221/ssoar-2020-epifanova-Deciphering Russias Sovereign Internet Law.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2020-epifanova-Deciphering Russias Sovereign Internet Law.pdf

[3] Splinternet: How Geopolitics and Commerce are Fragmenting the World Wide Web https://books.google.co.in/books?hl=en&lr=&id=vOF0CwAAQBAJ&oi=fnd&pg=PA7&dq=research+paper+on+splinternet&ots=SHj7nLGfUe&sig=9FttR55b9VrqP3

[4] Jessica Baker, Ph.D. "How Does GDPR Affect You?" Guardian of the Internet. http://blog.digitalguardian.com/what-does-gdpr-mean-for-you

[5] L.S. "What is the splinternet?" explains The Economist. The Economist is a publication that focuses on economic issues. https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet Bruce Sterling,

[6] "China's Splinternet Model is Working." Wired. https://www.wired.com/beyond-the-beyond/2016/07/china-splinternet-model-winning/

[7] Victor Tangermann. "With his decision on GDPR, Zuckerberg demonstrates that he has learned nothing from the Cambridge Analytica scandal." Futurism. https://futurism.com/zuckerberg-gdpr-cambridge-analytica/

[8] Pierre Tanguay, Sabrina Dubé-Morneau, and Galle Engelberts. "Splinternets: How Online Balkanization Is Making Digital Content Distribution More Difficult." Trends in CMF. https://trends.cmf-fmc.ca/splinternets-how-online-balkanization-is-creating-a-headache-for-digital-content-distribution/ (Last accessed September 2018).