The Indian EXPRESS

Explained: Why the Russia-Ukraine war threatens to splinter the internet

Splintering is the idea of splitting the internet into disparate realms controlled by different dispensations or powers. The events of the past four weeks pose the first serious challenge to the way the internet has evolved.

Written by Pranav Mukul, Anil Sasi
April 2, 2022 12:53:24 pm

The internet is essentially a global network of physical cables. The concept of the splinternet envisages blocks or regulation of these connections points.

In 2001, when the internet was staring at a slew of regulations from across the globe, Clyde Wayne Crews, a researcher at libertarian think-tank Cato Institute, proposed the idea of 'splinternet' — an internet splintered into disparate realms controlled by different dispensations or powers.

The fundamental proposal was to have more internets instead of having more regulations.

Over the past two decades, a splintering of internet has occurred in some limited ways. **China's 'Great Firewall'** keeps American tech giants out while pushing online services developed indigenously. Russia, in 2019, passed the sovereign internet law — or the online Iron Curtain — that enabled the country to disconnect its internet from rest of the world.

The splintering

Crews may have been ahead of his time in propounding a splinternet. But the events of the past four weeks pose the first serious challenge to the way the internet has evolved into a global system of interconnected computer networks, that use the Internet Protocol suite (TCP/IP) to communicate between networks and devices.

However dystopian the idea may have seemed over these years, Russia's invasion of Ukraine does seem as a potential trigger for a splintered internet. France's digital affairs envoy Henri Verdier, in an interview to *Bloomberg News*, recently stated that the combination of Moscow's increasing online censorship attempts, combined with Ukraine's repeated calls for Russia to be taken offline, could potentially offer the trigger for the eventual "fragmentation of the internet."

“Will the unique, neutral, multi-stakeholder, free internet survive this crisis?” Verdier asked. “I’m not sure.”

The internet is essentially a global network of physical cables, which can include copper telephone wires, TV cables, and fiber optic cables, alongside wireless connections such as Wi-Fi and 3G/4G, that leverage the physical cables to hook users and devices on to the internet. Countries hook on to global web services via undersea cables or nodes that are connection points through which data is transmitted to and from other countries’ communication networks. The concept of the splinternet envisages blocks or regulation of these connections points.

Viability barrier

Can Russia, or China, simply create a parallel or alternative system that will be viable? There are already experiments of government-managed walled gardens that are taking shape.

In Iran, for instance, a project called the National Information Network (NIN) — also known as National Internet in Iran — has been initiated by the state-owned Telecommunication Company of Iran. The Supreme Council of Cyberspace of Iran defines the NIN as “a network based on the Internet Protocol with switches and routers and data centers which allows for data requests to avoid being routed outside of the country and provides secure and private intranet networks”.

China’s ‘Great Firewall’, also known as ‘The Golden Shield Project’, is another experiment on these lines. It was initiated by the Ministry of Public Security division of the Chinese government in 1998. The focus of this project is to monitor and censor what can and cannot be seen through an online network in China, and is continually improving in restriction techniques through various methods. It blocks access to many foreign internet services, which in turn helps domestic tech giants, such as Baidu, to spread their reach.

Like Baidu, Russia already has tech champions such as Yandex and Mail.Ru. But unlike their Chinese counterparts, Russians have been able to access global tech platforms such as Facebook, Twitter and Google, albeit some censorship.

But in the years since its invasion of Crimea, Moscow has been proactively working on its segregated internet project. The country plans to create its own Wikipedia, and Russian legislators have passed a law that bans the sale of smartphones that do not have pre-installed Russian software.

Much of these provisions and restrictions on western platforms is being done through a “sovereign internet law” enacted by Moscow in 2019, that allows Roskomnadzor — a state owned communications player — to regulate internet access in the country and potentially cut its online ties to the rest of the world.

As sanctions tightened, Moscow said it had decided to block Facebook in retaliation to restrictions slapped by it on Russian media outlets.

India, too, is understood to be working on a new cybersecurity and data governance framework amid the continued “weaponisation” of the internet by Big Tech platforms during the Russia-Ukraine conflict, that put into focus the sweeping powers of social media platforms.

The groundwork and sandboxing for a splintered Indian internet has ostensibly been happening over the last few years. Just last year, Union ministers and political leaders from the ruling BJP put their weight behind the microblogging app **Koo** — it was at the same time New Delhi was in a kerfuffle with Twitter.

What are the problems with splintering?

So far, state-sponsored cyber-warfare, despite stray instances, has been a scattered occurrence. This has mainly been possible because of diplomatic involvement of countries and jurisdictions in maintaining cyber-relations. The splinternet could put a spanner in these works.

According to Verdier, any move by Russia to move toward an independent internet "would have severe consequences", including the temptation by countries to launch cyberattacks as they would be insulated from the impact.

"Today if I break the Russian internet, probably I will break my own internet, because it's the same," Verdier told *Bloomberg,* arguing the shared nature of the world wide web protected all users from losing service.

US President Joe Biden has already warned that Russia is considering attacks on critical infrastructure. "Based on evolving intelligence, Russia might be planning a cyber attack against us," Biden said at a press conference on March 21. "The magnitude of Russia's cyber capacity is fairly consequential and it's coming."

Moscow has categorically denied these accusations. "The Russian Federation, unlike many western countries, including the United States, does not engage in state-level banditry," Kremlin spokesman Dmitry Peskov said Tuesday.

Case for a splinternet

Crews had argued two decades ago that "warfare on the digital commons invites more regulation and adds to a deteriorating and antiquated internet". He had written that splintering the internet would not only increase the options but also protect the rights of internet users, "which depend so critically on the institution of private property".

It is also notable how a project for Bitcoin — a cryptocurrency developed in the aftermath of the 2008 financial crisis with the fundamental driver being lack of trust in a centralised authority — has evolved and culminated into propagation of Web 3.0, which is a reimagined and decentralised form of an open, trustless, and persmissionless internet, or perhaps, another splinter in the existing internet.