Cyber Frontlines

How India is Fortifying Its Digital Borders Amid Cross-Border Tensions

Aryaman Mann, TechSphere Insights,
May 2025, Volume 1, Issue 5, pp. 20–23.

As the world becomes increasingly interconnected, cyber threats have risen sharply, and countries have begun to consider cyberspace among the key domains of conflict. Especially in South Asia, the trend is clear: the cyberattacks spike with land or maritime tensions. The clash in the Galwan Valley in June 2020 is a prime example of the same. One security firm reported a 300% increase in Chinese cyber intrusions targeting Indian networks during that time. Similarly, whenever skirmishes with Pakistan intensified, India's Cyber Emergency Response Team (CERT-In) reported an increase in ransomware, DDoS, and malware attacks on government and business systems. As such, India has started to view its online infrastructure as a new and crucial border that needs to be protected. This means that India is now openly talking about tightening its digital sovereignty to ensure national security in the ever-developing world.

Groundwork

India's initial investment in cybersecurity started more than a decade ago. The Information Technology Act, 2000 (amended in 2008), laid the first legal groundwork against cybercrimes. In 2004, the government established the CERT-In as the national agency for incident response and security awareness. Over time, more institutional firewalls were built, like the National Cyber Security Policy that was released in 2013, and the National Critical Information Infrastructure Protection Centre (NCIIPC) was created in 2014 to secure important systems in the power and finance sectors.

But these measures weren't enough. In a report by India Today, it was revealed that around 1000 Indian government websites were hacked from 2009 to 2012. Not only that, but most of the attacks were on the heart of national security. Sensitive data from the Defence Research and Development Organisation (DRDO) network was leaked, and even the Prime Minister's Office website was infiltrated. Security experts warned that such incidents were the same as warfare and called for strengthened laws and measures, as well as international cooperation. In short, India had realised the real threat of cyber espionage by the mid-2010s.

Strengthening the Digital Border

From 2015 onwards, serious actions were taken for cyber defences in many pivotal areas. The government increased funding and attention for the same. For instance, the union budget 2023-2024 allocated ₹759 crores to cybersecurity projects and raised the CERT-In budget to ₹238 crores. Strategic initiatives were also taken. For example, India established the National Cyber Coordination Centre (NCCC) in 2017 to monitor internet traffic for any threats. Later, a National Cyber Security Coordinator was appointed to make the policies more efficient. CERT-in has been empowered by the government with mandatory reporting rules. Under recent changes, effective from 2022, all government telecom, cloud, and other critical service providers must report major incidents to CERT-In within hours and also maintain detailed activity logs.

Defensive infrastructures have also been strengthened, and special exercises have been formed to prepare for any future cyber conflicts. In October 2023, the National Security Council Secretariat organised a large-scale national cyber

exercise—the Bharat NCX 2023. It lasted for two weeks, and the “live-fire” drills brought together hundreds of participants to do simulation attacks on important information infrastructures. The exercise featured red-team versus blue-team war games and a CISO conclave with 200 top security officers. In order to address the ever-developing threats, Bharat NCX emphasised the necessity of thorough cyber strategies and tight public-private sector cooperation.

As the Chief of Air Staff has rightly said and highlighted that future battles might be fought in the digital realm, collaboration between stakeholders has become important and central to India’s approach. CERT-in routinely issues guidelines and alerts, one of the most recent being in early 2025, when it warned MSMEs about an increase in attacks due to India-Pakistan tensions. Memoranda of Understanding have been signed with many countries, including Singapore, Japan, South Korea, the United Kingdom, and more. This was done to exchange threat intelligence and best practices about the same. “Exercise Synergy” was hosted by CERT-In in September 2022 with Singapore’s Cyber Security Agency and 12 other countries, clearly emphasising the rise in international cooperation.

These initiatives are important, for it has been confirmed many times that cyber incursions have happened from state-linked adversaries. In April 2022, a media report detailed how Chinese-sponsored hackers had targeted seven regional electricity grid hubs near Ladakh, though these attempts were foiled. Security officials have continued to track active Pakistani and Chinese Advanced Persistent Threat (APT) groups trying to infiltrate and probe the Indian networks.

As such, strict actions have been taken. India has tightened its control over the cyber borders through various regulations and initiatives, for example, banning various Chinese apps like TikTok. One of the recent high-profile steps was the ban of several popular VPN apps, including Cloudflare’s 1.1.1.1, from Indian app stores. This was the first major implementation of a 2022 rule that clearly stated that VPN services are required to keep detailed user logs. While various industry and business groups disagreed with the changes, fearing security and privacy issues, it’s clear that the initiative reflects India’s drive for digital sovereignty. India's aim is transparent, that is, to maintain authority and safeguard encryption and data.

Looking Ahead

India is planning to have aggressive and ambitious upgrades to strengthen its digital borders even more. One essential point is the finalisation of a National Cyber Security Strategy, which has been repeatedly mentioned in recent policy discussions. The priority in such a strategy is to have a cohesive and unified vision for cyber defence, including legal structures and governance frameworks. At the Bharat NCX exercise, it was emphasised that transparent laws and public-private cooperation are crucial.

India is expected to use cutting-edge technologies for defence, including adopting AI and machine learning to automate attack detection and expanding Security Operations Centres (SOCs) for vital sectors. Not only that, but the government is also considering reforming cyber laws and updating the IT Act to battle the emerging challenges, which include financial internet crimes and stricter rules on the increasing social media misinformation propaganda.

The Finance Ministry has suggested that funding for cyber initiatives is likely to grow even further. Reportedly, plans are underway to set up more security training programs and research labs to lessen the dependency on imports. Cybersecurity will be integral to the vision of Secure India. Critical infrastructure protection will remain as one of the top priorities, as shown by India's aim to design strong networks for power, finance, telecom, and transport to battle various cyberattacks.

Besides the internal workings and changes, international cooperation will also shape India's digital border. India is reportedly negotiating detailed and dedicated agreements with partners, deepening bilateral and multilateral relations. In one of the recent reports, it's stated that India and Australia have begun talks on a "cyber pact" for faster data sharing and collaborative response to cyberattacks. There are many more such instances, which show that international cooperation is also on the high-priority list.

In summary, India's digital borders are being fortified through various sophisticated and diverse means, sharp policies and technology developments. The past decades have taught a brutal but eye-opening lesson to India; as such, the government has started to move aggressively to a greater, better, and stronger future. The new legal powers for CERT-In, bigger security budgets, international cooperation, and specialised exercises will ensure that India's crucial systems will remain secure in the constantly developing and contested cyberspace.