International Journal of Academic Excellence and Research (IJAER)
e-ISSN: 3107-3913 || Publication Impact Factor (I2OR) : 2.015
Vol. 02, No. 01, January-March, 2026, pp 113-119

www.mgmpublications.com

India's Digital Strike on Pakistan

Dr. Omkar Sonawane*
Assistant Professor, Department of Defence and Strategic Studies, Savitribai Phule Pune University.
***Corresponding author:** dromkarphd@gmail.com
Citation: Sonawane, O. (2026). India's Digital Strike on Pakistan. International Journal of Academic Excellence and Research, 02(01), 113–119. https://doi.org/10.62823/IJAER/2026/02.01.169

Abstract: *The recent tensions along the India–Pakistan border, following the Pahalgam terror attack on Indian soil has prompted the Indian Ministry of Information and Broadcasting to order urgent directives to all leading over the top platforms and digital content producers in India to ban digital content with Pakistan origins. Following which special advisories were issued on the grounds of national security and sovereignty. It is in this context that the paper analyzes India's digital strike on Pakistan and its implications on its bilateral relations. It also highlights how India has addressed such challenges proficiently within its digital realm and its response to Pakistan's disinformation efforts.*

Article History:
Received: 14 February, 2026
Revised: 24 February, 2026
Accepted: 04 March, 2026
Published Online: 08 March, 2026

Keywords:
Digital Strike, Operation Sindoor, Military Aggression, Bilateral Relations.

Introduction

On April 22nd, 2025, the Pakistan-based terrorist group, The Resistance Front[1] perpetrated a devastating terror attack in Pahalgam[2] in the state of Jammu & Kashmir, India. This attack caused the deaths of 26 innocent civilian including military[3] and intelligence[4] personnel, who were killed in cold blood. TRF, a Pakistani-based terrorist organization backed by Lashkar-e-Taiba[5], claimed responsibility for this attack. Post-attack, TRF took responsibility not once but twice. Similarly, Pakistan's denial to acknowledge such terror groups operating on its soil and neither the willingness to curb these terror-related infra-networks compelled the Indian Government to take decisive and punitive action against those held responsible.

It is in response to this escalation followed with public outrage, on the night of May 7– 8, 2025, the Indian Government executed Operation Sindoor[6]. The key aim of this operation was to precisely hit terror infrastructure networks, which targeted terrorist training camps at several locations inside Pakistan[7] and Pakistan Occupied Kashmir[8]. In response to these events on May 8th, 2025, Pakistan carried out a retaliatory military response by launching multiple drone and missile strikes targeting Indian military assets across the northern and western frontier. Similarly, drone attacks and munitions attacks were also carried out in civilian areas that include Srinagar, Jammu, Pathankot, Amritsar, Ludhiana, Bathinda and Bhuj.

India's robust counter-drone grid and layered air defense systems well anticipated these incoming aerial threats, and the recovered debris from these drones and ammunitions were inconclusive to its origins to Pakistan and China[9]. Following these provocations, India conducted further strikes with precision-guided weapons against Pakistani Air Defense Systems at several locations inside Pakistan. These missile strikes were confined only to neutralizing Pakistani Air Defense Systems that facilitated earlier aggression and were executed under the principle of 'equal intensity in the same domain.' Thus, India balanced the imperative of deterrence without overstretching its commitment to de-escalation.

India-Pakistan Conflict

The India–Pakistan (2025) conflict was a brief four-day armed conflict between the two nuclear-armed nations that began on May 7th, 2025. After which India launched missile strikes on Pakistan and Pakistan Occupied Kashmir in a coordinated military operation. The entire operation lasted for twenty-two minutes, giving a swift response to Pakistan. India mentioned that the operation was carried out in response to the Pahalgam terrorist attack in the state of Jammu and Kashmir on 22nd April 2025, because of which twenty-six innocent civilians were killed[10]. India accused Pakistan of supporting cross-border terrorism, which Pakistan denied. Soon, India launched Operation Sindoor to destroy Pakistani - sponsored terrorist infrastructure. Those affected militant groups include Jaish-e-Mohammed[11] and Lashkar-e-Taiba.[12]

The intention behind these strikes were clear and have said not to be hitting any Pakistani civilian facility, but a surgical strike on Pak-sponsored terrorism. However, Pakistan refutes these claims and mentioned that the missile strikes hit hard in civilian areas, resulting in civilian casualties. As a result of these missile strikes, border skirmishes between the two nations began, followed by drone strikes on each other. The Pakistani Army further launched a blitz of mortar shells on civilian areas such as the Jammu Region, in particular Poonch district, attempting to cause civilian casualties and damage civil infrastructure. On May 10th, 2025, India accused Pakistan of launching missile attacks on its air bases, including the Sirsa Air Base, while Pakistan accused India of launching attacks on its air bases, including Chunian, Murid, Nur Khan, Pasrur, Rafiqui, Rahimyar, Sargodha, Shahbaz, Sialkot, Skardu and Sukkur Air Bases. As the conflict escalated, Pakistan launched its Operation Bunyan-un-Marsoos, which was said to have targeted several Indian military installations, with no reported damages. Similarly, on May 10th, 2025, a hotline was established between the Director Generals of Military Operations (DGMO) and both nations agreed upon a ceasefire, ending the brief military confrontation.

Key Fallout of India-Pakistan Conflict 2025

- Termination of the Indus Water Treaty.
- Closing of Attari-Wagah Border.
- Suspension of Bilateral Trade.
- Revoked Visa of all Pakistani nationals residing in India.
- Ban on Pakistani Artists.
- Punishment via Military and Non-Military measures.
- Operation Sindhoor. (Strategic Planning and Targeted Response)

Digital Sanctions Against Pakistan

In response to the Operation Sindoor, the Indian Ministry of Information and Broadcasting issued an urgent advisory asking all over-the-top platforms and online media-streaming platforms in India to discontinue web series, films, songs, podcasts, and other media content of Pakistani origin with immediate effect.[13] "Several terrorist attacks in India have had cross-border linkages with Pakistan-based state and non-state actors. Recently, on April 22, the terrorist attack in Pahalgam led to the killing of several Indians, one Nepali citizen, and injuries to several others," it said.[14]

The Ministry quoted Part-III of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, which provides for a code of ethics for publishers of online content. The government emphasized that publishers must avoid content falling under the following categories:

- Content affecting the Sovereignty and Integrity of India.
- Content that Endangers State Security.
- Content that is likely to Incite Violence or disturb Public Order.

The Ministry invoked Rule 3(1)(b) of the IT Rules, 2021, which mandates intermediaries to take reasonable steps to prevent the hosting or transmission of content that threatens India's unity, integrity, defense, or sovereignty.[15] The list of banned YouTube channels includes; BOL News, Geo News, The Pakistan Reference, Samaa Sports, GNN News, Uzair Cricket, Umar Cheema Exclusive, Razi Naama, Raftar TV, Dawn News, ARY News, Samaa TV and Suno News.[16] In addition, the blocked social media handles of Pakistan Artists include; Saba Qamar, Ahad Raza Mir, Danish Taimoor, Hasan Ali, Ali Zafar, Bilal Abbas, Iqra Aziz, Ayeza Khan, Imran Abbas, Yumna Zaidi, Irshad Bhatti, Asma Shirazi, Muneeb Farooq, Mahira Khan, Fawad Khan, Mawra Hocane, Hania Amir, Shahid Afridi, Babar Azam, Mohammad Rizwan, Wasim Akram, Shan Masood, Sanam Saeed, Naseem Shah, Imam-ul-Haq, Shadab Khan and

Shoaib Akhtar remain blocked in India.[17] Similarly, Pakistani TV shows no longer appear on Indian OTT platforms' catalog and many YouTube channels of Pakistani broadcasters that were streaming Pakistani TV series stand banned in India, as per previous government orders.

YouTube Monetization Scheme

The YouTube monetization scheme enables creators to earn money by joining its YouTube Partner Program. This program provides revenue streams through adverts, paid memberships and commission on YouTube shopping. At entry level, content creators need at least 500 subscribers, with videos being uploaded for the past 90 days. To unlock revenue and monetize schemes, channels must reach 1,000 subscribers or have 4,000 hours of valid public watch time in the last 12 months. Participating channels must comply with their guidelines. Monetization works through an automated system review. When creators turn on monetization for their videos, YouTube checks whether the content is compliant and advert friendly. If creators violate guidelines, such as uploading inauthentic content or breaking rules, monetizing YouTube videos may be suspended, resulting in significant damage to the content creator. The scheme thus supports a range of earning methods, but emphasizes authentic, original content, along with compliance and policy updates.

Ban Impact.

The digital subscriber base always acts as its key advantage for any digital application and content creators who create and upload content on digital streaming platforms. Along with providing millions of viewership and generating revenue through application downloads, the application developers' firms also get access to individuals' data and personal information using such applications. They often generate revenue through application downloads, in-app digital advertisements, paid digital subscriptions, sponsorships, in-app purchases, adverts, and other peer-to-peer monetary transactions.

Given the fact that India has around 900 million active internet users, the recent ban of digital content against Pakistan has acted as a major setback to Pakistan's disinformation efforts. Particularly in relation to the defamation of the National Defence Forces. The banning of Pakistani digital content hosted on popular streaming apps has put pressure on Pakistani artists and content creators to create content that is free of any misinformation or disinformation. For instance, the popular Pakistani cricketer Shohaib Aktar has his own YouTube channel known as '100mph' which stands blocked for propagating misinformation against India[18]. Its primary source of revenue came from a large number of subscribers, online viewership and internet fan following.

Meanwhile, in response to this digital ban, Pakistan has pulled off Indian music from its radio stations. Songs of legendary singers like Lata Mangeshkar, Kishore Kumar and popular artists like Arijit Singh and Shreya Ghoshal that were dominating Pakistan's radio stations have been discontinued.[19] Pakistan's Information Minister, Attaullah Tarar, quoted, "This decision shows a strong sense of national solidarity on behalf of the Pakistan Broadcast Association. I deeply appreciate the initiative of the PBA on its own, which upholds the dignity and sovereignty of the nation. This shows we all stand united in promoting national unity and supporting core values during such testing times." [20]

Enforcing Digital Ban; India's Legal Framework

The regulation of cyberspace has become a complex task because of the growing integration of economies and blurred boundaries of the global markets. Therefore, the legal framework to govern such advanced forms of communication like digital applications and over the top content platforms that create and store information is key to protecting nation-states. Thus, India has devised an elaborate framework that not only govern cyber space, social media and over the top content platforms but simultaneously addresses the threats and challenges being faced in its digital spectrum. The following are the legal and institutional frameworks that play a critical role.

Section 69A

Section 69A of the Information Technology Act, 2000 grants the central government with authority to take legal action against any information that threatens the country's sovereignty, integrity, defense, security of state or public order. Section 69A gives the government the authority to block any content from public access. Section 69A states that if any online content threatens the integrity and

sovereignty of the country or affects its relationship with friendly foreign countries, then it can enforce a ban against such content under this section. The procedures are mentioned under the IT (Procedure and Safeguards for Blocking Access of Information by Public) Rules 2009. Intermediaries that fail to comply with blocking orders can face punitive action. The government is entitled to the following powers under Section 69A:

- To issue directives to remove objectionable content on social media platforms.
- To punish concerned authorities for failing to comply with orders directed by the Central Government.
- To grant the Central Government authority, to invoke section 69A to protect the dignity of the constitutional institutions of the country.

Information Technology Act (2000)

The Indian Parliament passed the Information Technology Act (2000) and the Ministry of Electronics and Information Technology administers this act. Originally, the Act was developed to promote the IT industry, e-commerce, and practice global security standards. The Act was amended in 2008 and 2023 to address issues that the original act failed to cover. The Act in total has 13 chapters and 90 sections and applies to the whole of India. The act also applies to offences which are committed outside the Indian Territory affecting the Indian cyberspace.[21]

Ministry of Information and Broadcasting

It is a vital ministry that represents the face of the government in its outreach to the masses. The Ministry is entrusted with disseminating information about government policies, schemes and programs through different modes of mass communication. This includes radio, television, press, social media and printed publicity. The Ministry is also the focal point on policy matters regarding private broadcasting, public broadcasting, multi-media advertising, and publicizing policies of the government. It oversees matters that pertain to All India Radio Service and Doordarshan through the Broadcasting Corporation of India Act 1990.[22] during Operation Sindoor, the MIB was responsible for blocking over 1,400 URLs on various social media platforms. These URLs were indulged in spreading false, misleading, communally sensitive and anti-India content.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, notified by Ministry of Information and Broadcasting sets a Code of Ethics for digital media focusing on online safety, content removal and establish grievance redressal system for Digital Media and OTT Platforms along with Strict Rules for Social Media Intermediaries.[23]

For Intermediaries (Social Media) includes;

- Intermediaries must publish rules, appoint grievance officers, and take down harmful content.
- Publish compliance reports and contact details of the intermediaries.
- Appoint self-regulatory organizations and oversight mechanisms. (Three tier system)

For Digital Media (OTT Platforms) includes;

- OTT platforms must classify content and implement digital locks for age-appropriate content.
- Exercise digital restraint on content impacting the nation's sovereignty and cultural sensitivities that affect public order.

Press Information Bureau

The Ministry of Information and Broadcasting, under the Government of India (Allocation of Business) Rules, 1961, is responsible for disseminating information on government policies, schemes, and programs through various modes of communication. It has several subordinate offices, including the Press Information Bureau. It is the nodal agency of the Government of India and is primarily tasked with information dissemination to print and electronic media on government policies, programs, initiatives and

achievements. This includes press releases, press notes, factsheets, articles, photographs, videos and infographics. It functions as a key interface between the government and media and provides feedback to the government.[24]

Press Information Bureau Fact Check Unit

The PIB Fact Check Unit is the forefront organization in tackling fake news related to the Government of India. The PIB-FCU was established in the year 2019 to tackle fake news related to central government, its ministries, departments, public sector undertakings and other central government organizations. This unit verifies claims on government policies, announcements and regulations through rigorous fact-checking procedures. This unit helps to dispel rumors, myths, and false narratives by providing accurate and reliable information. The unit's operations are carried out by IIS cadre officers and is headed by a DG-level officer of the Indian Information Service. The FCU reports to the Principal Director General, PIB, who functions as the Principal Spokesperson to the Government of India.[25]

During Operation Sindoor, the PIB-FCU played a critical role in dispelling misinformation on major social media platforms. The Unit debunked Pakistani propaganda against India and the Indian Armed Forces and fact-checked posts to counter any misinformation. A special control room was established with inter-departmental coordination to facilitate real-time information among all stakeholders. This control room comprised nodal representatives from the Indian Army, Navy and Air Force, along with officers from various government media units.

Proactive Approach Taken by PIB- Fact Check Unit Includes

- Discrediting sources by exposing manipulation tactics used by Pakistan-based social media accounts to spread disinformation.
- Promoting media literacy via an educational campaign to educate citizens on identifying fake narratives.
- Effectively communicate on behalf of the Government of India.

Ministry of External Affairs Fact Check Unit

Though the Ministry of External Affairs[26] does not have any independent fact - check unit, it relies upon the Press Information Bureau Fact Check Unit which is mandated to debunk misinformation regarding all Government of India Ministries. The ministry uses its official social media handle along with the PIB's infrastructure in order to clarify facts regarding international matters, fake news and visa-based rumors. The ministry plays a crucial role in its fight against disinformation at home and abroad.[27]

Ministry of Electronics and Information Technology

In 2016, the Ministry of Electronics and Information Technology was created and became the single agency responsible for IT policy, strategy, and the development of the electronics industry. Its major responsibilities include promoting IT industries, e-governance, growth of electronics, and enhancing internet governance. The Ministry is headed by the Central Minister and is the nodal agency for India's IT and communication sector. Prominent agencies that fall under this ministry include; Cyber Appellate Tribunal and Computer Emergency Response Team.[28]

Indian Computer Emergency Response Team

Computer Emergency Response Team is a cyber-security organization that comes under the Ministry of Electronics and Information Technology, Government of India. It is responsible for implementing the Information Technology Act, 2000. It is mandated to deal with computer-related incidents in India. The Director General of CERT heads this organization. The agency deals with cybersecurity threats such as phishing, smishing, vishing, viruses, malware, and critical infrastructure. Besides collecting and analyzing data, the agency does forecasts and advises the government on upcoming cyber threats. It is also responsible for strengthening India's internet domain.[29]

Ministry of Home Affairs

The Ministry of Home Affairs is responsible for the maintenance of internal security in India. Apart from maintaining internal security, it also deals with border management, terrorism[30], intelligence, multi-agency center, center-state relations, and administers Union Territories. Under Article 355 of the Indian Constitution, it is the duty of the Union to protect its states against external aggression and internal disturbances. The Ministry ensures that every state government follows the constitution's provisions. Since public order and police come under the State List, it assists state governments by providing them with central armed police forces and financial support towards police modernization.[31]

National Cyber Coordination Centre

It is the nodal agency that comes under the Ministry of Home Affairs, Government of India. It was created in the year 2017 with the intent to deal with malicious cyber threats and act as an internet traffic monitor. Key components of NCCC include; e-surveillance, network monitoring, information sharing, review laws and plan cybercrime prevention strategy. The government set up the NCCC in order to mitigate threats related to cybercrime and national security while working in close coordination with the country's top intelligence agencies such as NTRO, CBI, IB and RAW. This agency also acts as an internet traffic monitor against incoming cyber threats, both domestic and international.[32]

Indian Cybercrime Coordination Centre

Indian Cybercrime Coordination Centre is an initiative of the Ministry of Home Affairs, Government of India, to deal with cybercrime within the country. It mainly focuses on issues related to cybercrime by providing coordination between citizens and law enforcement agencies. The I4C scheme was formally approved by the Ministry of Home Affairs in 2018 and has strived towards enhancing the nation's cyber defense capability by tackling cybercrime since 2020.[33]

Key I4C Objectives;

- Act as a nodal point to curb cybercrime.
- Generate awareness to prevent cybercrime.
- Facilitate an easy process to file cybercrime complaints.

Conclusion

Thus, the digital strike carried out against Pakistan by banning digital content on OTT platforms and popular streaming apps marks a noticeable shift in India's stern approach towards Pakistan and at the same time implies firm self-determination in its national security matters. India as a country has effectively leveraged its digital spectrum to punish Pakistan and its state-sponsored terrorism by effectively blocking digital content and its content creators for those who were found in violation of Indian cyber laws and its codes of ethics. The skirmishes between the two nuclear-armed nations remind one that India is no longer submissive to cross-border terrorism and neither does it fall prey to tactics of misinformation.

References

1. https://indianexpress.com/article/india/trf-published-photo-pahalgam-attack-site-twice-claimed-responsibility-unsc-sanctions-report-10158894
2. https://icct.nl/publication/operation-sindoor-turning-point-india-addressing-terrorism-kashmir
3. https://www.thehindu.com/infographics/2025-04-24/pahalgam-terror-attack-victims-tribute/index.html
4. https://www.ndtv.com/india-news/intelligence-bureau-officer-manish-ranjan-shot-in-front-of-wife-kids-in-pahalgam-terror-attack-deaths-8230390
5. https://main.un.org/securitycouncil/en/sanctions/1267/aq_sanctions_list/summaries/entity/lashkar-e-tayyiba
6. https://www.cgiistanbul.gov.in/section/news/summary-of-operation-sindoor

7. https://www.thehindu.com/news/national/operation-sindoor-full-list-of-terrorist-camps-in-pakistan-pojk-targeted-by-indian-strikes/article69547986.ece
8. https://www.satp.org/islamist-extremism/data/The-Northern-Areas-of-Pakistan-Occupied-Kashmir
9. https://www.indiatoday.in/sunday-special/story/india-pakistan-war-will-shape-future-battles-chinese-weapons-operation-sindoor-brahmos-sukhoi-rafale-pl-15-2726349-2025-05-18
10. https://www.theguardian.com/world/2025/apr/22/tourists-killed-by-suspected-militants-in-kashmir-attack
11. https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organizations/listed-terrorist-organizations/jaish-e-mohammad
12. https://www.efsas.org/publications/study-papers/al-qaeda,-is-and-lashkar-e-taiba-modus-operandi-in-south-asia-and-europe
13. https://www.bwmarketingworld.com/article/mib-orders-immediate-ban-on-pakistan-origin-content-across-ott-platforms-556185
14. ibid
15. ibid
16. https://www.newsonair.gov.in/india-bans-16-pakistani-youtube-channels
17. https://timesofindia.indiatimes.com/city/delhi/full-list-of-pakistani-actors-whose-instagram-accounts-are-still-visible-in-india/articleshow/120788982.cms
18. https://timesofindia.indiatimes.com/sports/cricket/news/shoaib-akhtars-youtube-channel-banned-in-india-following-pahalgam-terror-attack/articleshow/120687468.cms
19. https://www.hindustantimes.com/india-news/pakistan-fm-stations-stop-airing-indian-songs-as-tensions-with-india-rise-101746118170245.html
20. https://www.instagram.com/reel/DJHmIB_sKrV/?hl=en
21. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
22. https://mib.gov.in
23. https://mib.gov.in/documents/notification/acts-policy-guidelines
24. https://www.pib.gov.in
25. https://www.pib.gov.in/FAQ_fact
26. https://www.mea.gov.in
27. https://x.com/MEAFactCheck
28. https://www.meity.gov.in
29. https://www.cert-in.org.in
30. https://www.mha.gov.in/sites/default/files/PRAHAAREng_23022026.pdf
31. https://www.mha.gov.in
32. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474&reg=3&lang=2
33. https://i4c.mha.gov.in/about.aspx.

❑❑❑