

# Cross-Border Cyber Threats: Pakistan's Digital Activity Against India

Deepak Sagar<sup>1</sup>, Dr. Yasharth Gautam<sup>2</sup>

<sup>1</sup>Senior Research Fellow, Department of Defence and Strategic Studies, Bareilly College, M.J.P. Rohilkhand University, Bareilly, (U.P.), India.

<sup>2</sup>Assistant Professor, Department of Defence and Strategic Studies, Bareilly College, M.J.P. Rohilkhand University, Bareilly, (U.P.), India.

## Abstract

In the digital age, the Kashmir conflict turned into an information war, where stories were used as weapons. After the Pahalgam terror attack on April 22, 2025, India launched Operation Sindoor to attack terror camps in Pakistan and Pakistan-occupied Kashmir. At the same time, cyberspace turned into a battlefield. Over 2 lakh attempts – Targeting mainly power systems and government networks, Pakistan-linked hacker groups such as Advanced Persistent Threats (APT36) and SideCopy used fake websites, phishing emails and malware to steal data and disrupt services. Social media was also flooded with fake news, deepfakes and old data leaks to spread fear and confusion. Although these attacks caused little actual damage, they were aimed at undermining public confidence and creating panic. Similar cyber tactics have been seen in other conflicts such as Russia-Ukraine and Israel-Hamas. In response, India strengthened its cyber security, issued alerts and increased fact-checking. This shows that modern wars now involve digital attacks alongside conventional military action.

This paper assesses Pakistan's anti-India cyber activities and strategies, including technical attacks, attempts to influence public opinion through disinformation, and cyber activities during the Pahalgam attack and Operation Sindoor.

**Keywords:** cyber security, information warfare, cyberspace, India-Pakistan conflict

## INTRODUCTION

Cyberspace has emerged as a crucial battlefield in the changing conflict landscape of the 21st century—where bytes of bullets are fired, nations' security systems are breached, and stories are created, instead of physical weapons. The age-old rivalry between India and Pakistan, defined by conventional wars and border skirmishes, has now expanded to the digital realm. What was initially limited to hacking of webpages and low-level cyber-attacks has now evolved into an advanced strategy of online espionage, deceptive propaganda, and psychological warfare.

On 7 May 2025, the Indian Armed Forces launched Operation Sindoor, under which they carried out precision strikes to destroy terrorist hideouts in Pakistan and Pakistan-occupied Kashmir.<sup>1</sup> The operation was carried out in the wake of the terror attack in Pahalgam in which 26 tourists were brutally killed. The Indian Defence Minister said that the Indian Armed Forces carried out a precision military crackdown on

terrorist strongholds operating inside Pakistan so that these organisations do not dare to carry out violent incidents like Pahalgam in the future.

### Literature review

Cyber warfare is no longer a subset of traditional military conflicts but has become an independent and decisive battlefield. The use of digital modes in India-Pakistan tensions has not only transformed the nature of information but has also deeply affected democracy, infrastructure and strategic balance. This review brings out the various dimensions of this conflict through major research and reports from the last five years. The paper “Cyber Warfare Between Pakistan and India: Implications for the Region” by Dr. Ghulam Mustafa et al (2020) presents how both nations are now adopting cyberspace as a “low-risk offensive tool” away from traditional military confrontation. The article concludes that this shift takes South Asian regional security to a new and destabilizing turn. Sameer Patil’s (2022) ORF analysis “Pakistan Emerges as China’s Proxy Against India” explains how Pakistan, with the support of China, is challenging India as a cyber proxy. The article highlights APT groups, disinformation campaigns, and cyber espionage as threats to India’s democratic fabric. Prashant Mali’s (2025) research published in IJFMR, India’s Cyber Warfare Options Against Pakistan: A Strategic Analysis, presents an in-depth analysis of India’s cyber strategies, examining EMP weapons like KALI, vulnerabilities in Pakistan’s energy infrastructure, and influence of countries like China–Iran–Turkey from a strategic perspective. In the backdrop of Operation Sindoor, Usaid Siddiqui’s (Al Jazeera, 7 May 2025) article Information war: Are India and Pakistan telling the truth about attacks? Shows how information warfare emerged as a parallel strategic weapon between India and Pakistan, where rival nations engaged in narrative-control through social media and government statements. Reports by The Telegraph (May 5, 2025) and Times Now (May 13, 2025) reveal details of 1 million and 1.5 million cyber-attacks respectively, while a report titled “Road of Sindoor” by Maharashtra Cyber details the role of Pakistan-backed APT groups. Gauri Ramakrishnan’s (CAPS, May 20, 2025) analysis of the article Cyber Warfare: Dual Operational Fronts in Contemporary India-Pakistan Conflicts reinforces this dual front concept – where cyber aggressors and disinformation campaigns targeted India’s infrastructure and social systems in parallel with conventional military attacks. The article Operation Sindoor and India’s Cyber Threat Landscape by Patil (ORF, May 28, 2025) identified the role of the APT-36 group, malware like Crimson RAT, and global disinformation strategies as major threats to India’s national digital security. The developments reported by Madhuparna Das (NEWS18, June 24, 2025) show how India neutralised DDoS attacks originating from China and Pakistan in real-time with the help of MeitY and CERT-In. The report by Financial Express (June 15, 2025) critically examines the bizarre claim by Pakistan’s defence minister that floodlights of an IPL match were turned off by a cyber-attack—which was later established to be disruptions caused by an air raid alert.

### Research Methodology

This research uses qualitative and analytical methodology to examine the evolution and scale of Pakistan’s cyber rivalry activities towards India. It examines Pakistan’s malicious cyber activities in the aftermath of Operation Sindoor by India to understand how traditional conflict has transformed into a digital rivalry. Using content analysis, the study reviews government cyber advisories, cyber security reports and media reports to understand the nature and strategic nature of cyber-attacks and disinformation operations. To place India–Pakistan cyber competition in a broader geopolitical context, the research adopts a

comparative approach, including parallel analysis of cyber operations during the Russia–Ukraine and Israel–Hamas conflicts. This comparison helps to understand shared strategies and evolving trends of cyber warfare globally. The study draws on theoretical frameworks such as hybrid warfare theory, cyber-incitement model and information warfare, which provide intellectual foundations for explaining the practical developments and strategic objectives of cyber operations.

**1. Research Questions**

How did Pakistan use cyber-attacks and online disinformation against India before and during Operation Sindoor, and what were the impacts of these activities on India’s security and public?

**2. Hypotheses**

Cyber-attacks by Pakistan were not only technical but also part of psychological and information warfare.

**3. Objectives of the Study**

- To conduct a stratified analysis of Pakistan’s cyber-attacks against India during Operation Sindoor.
- To examine the role of Advanced Persistent Threat (APT) groups, disinformation networks, and cyber warfare in shaping the digital conflict.

**4. Data Collection**

- **Primary Sources:** The study is based on official advisories issued by CERT-In, PIB, and MAITI; Based on inputs from cyber security agencies like Maharashtra Cyber and Cyfirma and OSINT tools for monitoring hashtags, bot activity and disinformation trends on social media
- **Secondary sources:** This includes academic literature focused on cyber warfare, hybrid conflict and digital disinformation as well as credible reports from Financial Express, ORF, Reuss.

**Results**

A sharp increase in Pakistan’s cyber activities was witnessed with Operation Sindoor launched by India after the April 2025 Pahalgam terror attack. Hacker groups linked to Pakistan launched a number of cyber-attacks on Indian institutions, though none of them caused any significant disruption. Such attempts were seen several times after the Pahalgam attack and even before the escalation of the conflict, where operations of websites linked to the armed forces were disrupted. Despite this fact, these intrusions were successfully neutralised by the concerned agencies. The increase in cyber-attacks mirrors the pattern seen in the Russia-Ukraine conflict in Europe and the Israel-Hamas conflict in West Asia.

**Table: Cyber campaign against India by Pakistan after Pahalgam attack**

Campaign/Incident	Attack Type	Response
1. Pakistani cyber criminals targeted several government websites in Rajasthan	Web pages were defaced with anti-India messages	Adequate measures were taken and the website was temporarily shut down. <sup>2</sup>

<p>2. Cyber-attacks by Pakistani groups have been carried out on the websites of four defence establishments, two Army Public Schools, Srinagar and Ranikhet, Army Welfare Housing Organisation database and Indian Air Force Placement Organisation.</p>	<p>Attempts to deface web pages and networks</p>	<p>Quick Fixes by Web Managers.<sup>3</sup></p>
<p>3. Cyber-attack on India's power grid<sup>4</sup> and AI-created fake video of External Affairs Minister S Jaishankar apologising circulated<sup>5</sup>.</p>	<p>Part of wider impact operations</p>	<p>PIB and PTI denied the claim and called it fake</p>
<p>4. Pro-Pakistan social media handle falsely claims that Indian woman Air Force pilot Squadron Leader Shivani Singh was captured in Pakistan</p>	<p>Attempts to spread misinformation through fake domains</p>	<p>PIB denied the claim and called it fake.<sup>6</sup></p>

**Source: Online Print Media**

Cyber warfare can primarily be defined as -

“The activity of attacking computers in a country using the Internet, with the aim of damaging things like communication and transportation systems or water and electricity supplies.”<sup>7</sup>

Computer networks of government and private organizations, financial networks, power plants, etc. are all potential targets that cyber hackers can easily identify and distort or destroy to cause havoc. Manipulation of systems through spy software, stealing classified files, erasing data, rewriting web pages, inserting viruses, etc. are some of the examples of how hackers can infiltrate secure systems.

Beyond land, air, sea and space, there is another domain, the fifth domain, cyberspace, which is as strategically important as the four other domains of war where modern conflicts are fought. The Russia-Ukraine conflict is a prime example of this, where numerous cyber-attacks were carried out by state-backed and independent hackers on both sides. Similarly, there was a sharp increase in the number of cyber incidents during the initial phase of the Israel-Hamas conflict. Although these cyber operations have so far failed to cause any major damage, it would be a strategic mistake to underestimate the importance of such operations based only on the results.

Scholars have long debated the role of increased cyber operations during military crises and doubts have been raised about the role of cyber operations in escalating crises and malicious activities in cyberspace, which can lead to armed conflict.<sup>8</sup> It is also argued that cyber operations can be seen as an effective weapon even without being involved in armed conflicts. Moreover, considerable damage can be inflicted on the enemy without direct combat. Given the nature of cyberspace, it is argued that cyber weapons need to be used with great discretion as they can cause destruction comparable to that of nuclear weapons.

### **Cyber Strategy of Pakistan**

This aggressive strategy of Pakistan in the cyber sphere can be seen in the form of Advanced Persistent Threat (APT) and hacker group activity, disinformation through social media platforms and online activities by terrorist groups. Pakistan-backed APT groups have actively targeted Indian institutions, attempting to harm India’s interests. For example, Pakistan Cyber Force, cyber bunch HOAX1337 and National Cyber Crew<sup>9</sup>, APT 36 or Transparent Tribe, a Pakistan-linked threat group, has been active since 2013,<sup>10</sup> and has primarily targeted Indian defence, government and diplomatic institutions.

APT36 is based on Crimson RAT, a remote access trojan used for data exfiltration and espionage. The malware often mimics Indian government websites to distribute its malware. After the Pahalgam attack, APT36 launched a cyber-attack on Indian government institutions, Ministry of Defence and other organisations by defacing and destroying PDF files with a “Pahalgam terror attack” theme, which could be used to spread misinformation and conduct espionage.<sup>11</sup>

Another Pakistani APT group, SideCopy, has also been in the news for repeatedly sending phishing emails to Indian government institutions and targeting them with malware by creating fake domains of official services of India. During the conflict, Indian agencies identified some APT groups operating against India who were also responsible for more than 15 lakh cyber-attacks.<sup>12</sup> Most of these attacks reportedly originated from Pakistan, Bangladesh and the West Asian region. However, these groups are not as technologically advanced as Chinese APTs, which leverage zero-day exploits and conduct supply-chain attacks.

Various government agencies have flagged these activities and made security suggestions. India has taken measures to secure its critical infrastructure and sensitive assets, including energy, defence manufacturing, telecommunications and transport, and measures to enhance infrastructure are also being evaluated by the Department of Telecommunications. On May 10, an advisory was issued outlining the measures needed to keep MSMEs safe,<sup>13</sup> followed by separate instructions for large industries. Along with this, the agencies also warned of an increase in ransomware attacks, DDoS incidents, malware infections and web defacement.

However, hacker groups were less directly active and their involvement was also found to be low. Most of the information and misinformation was disseminated through social media. Most of which proved to be insignificant. Many of these groups belonged to other countries.

Nevertheless, they fuelled misinformation campaigns at a time when uncertainty about the crisis was widespread. The aim was to spread misleading, deceptive or biased information, typically through troll accounts, automated bots and coordinated mass messaging on platforms such as Twitter, Facebook and WhatsApp.<sup>14</sup> Manual count shows that the Press Information Bureau (PIB) released multiple fact-checks over five days to counter this tsunami of misinformation.<sup>15</sup> It also claimed that an Indian fighter jet Sukhoi Su-30MKI was shot down in Pakistan-occupied Kashmir (POK) and that an Indian pilot was captured. PIB Fact Check found that the image being used showed a Sukhoi jet that crashed in Maharashtra in 2014. These false stories, deepfakes, fake and edited images and documents and fabricated news articles were circulated globally using hashtags. Many experts inadvertently supported this misinformation without checking, which shows that even experts sometimes get caught in the tsunami of false information. After this, the Ministry of Electronics and Information Technology issued orders to block 8,000 accounts of social media platform X.<sup>16</sup>

Pakistan’s use of terrorism against India is not restricted to traditional domains. Terrorist organisations such as Lashkar-e-Taiba and Jaish-e-Mohammed have extensively used cyberspace to recruit, propagate, communicate, fund, plan and execute attacks. The Internet and social media platforms—including Facebook, Twitter, WhatsApp, Telegram and YouTube—have been effectively used to spread extremist ideology and recruit followers<sup>17</sup> Private social media and encrypted messaging apps have become an important means for organisations such as Lashkar-e-Taiba and Jaish-e-Mohammed to communicate and make secret plans. These organisations have also organised online and offline workshops to spread their ideology and objectives, incite youth in the Kashmir Valley to join violent protests against India and to

provide information about the cyber space. Lashkar-e-Taiba uses online game Age of Jihad to recruit youth.

Despite the temporary lull in conventional conflicts, reports continue to emerge that Indian government infrastructure continues to be vulnerable to hostile cyber-attacks. These cyber intrusions not only highlight the current vulnerabilities of institutional networks but also the changing definition of modern warfare.

### Discussion

This study makes it clear that Pakistan's cyber strategy is no longer limited to direct attacks but has taken the form of integrated and multi-layered digital warfare. The aim of cyber-attacks and disinformation campaigns was not only to cause technical damage but also to influence India's morale and public perception. India's resistance was comparatively balanced and strategic, with an emphasis on strengthening cyber security measures, preventing false rumours on social media and taking retaliatory action as needed. This example shows that cyber warfare has become an important dimension in today's wars, which needs to be understood not only from a technical but also strategic and social perspective.

### Conclusion

The recent cyber-attacks on India have made it clear that cyber threats are possible before, during, and after conventional military conflict. As soon as the news of the Pahalgam attack broke, hackers started targeting Indian government systems in a rapid manner. Cyber groups like SideCopy and APT36 created fake websites that looked like real government portals, and malicious software was sent through them, posing a threat to the security of the government and defence personnel. Also, rumours and misinformation were deliberately spread on social media to undermine people's trust in the government. However, the Indian government acted promptly and thwarted many of these attacks in time. Government official accounts on platforms like X (Twitter) played a key role in identifying fake information and removing accounts spreading false information. Still, the threat is not completely over. There is a need to be vigilant against attacks such as phishing emails, duplicate mobile apps, invisible spyware, and malware hidden on webpages. To deal with these threats, constant vigilance, strong cyber security measures and digital awareness among citizens are extremely necessary. The attack on India makes it clear that in today's times, digital attack has also become an important part of modern warfare. To protect against this, along with a fast government response, it is necessary to make the common people aware of cyber security.

### References

1. Debanish Achom, "The 9 Terror Targets In Pak Hit By India And Their Key Details" 07 May 2025. <https://www.ndtv.com/world-news/operation-sindoor-the-9-terror-targets-in-pakistan-hit-by-indian-missiles-and-their-key-details-8355768>
2. Neha Khan, "Pakistani cybercriminals hack three websites of Rajasthan govt", *The Siasat Daily*, 29 April 2025. <https://www.siasat.com/pakistani-cybercriminals-hack-three-websites-of-rajasthan-govt-3213875/>
3. "Cyberattacks by Pakistan groups on 4 defence facilities thwarted", *The Hindu*, 30 April 2025. <https://www.thehindu.com/news/national/cyber-attacks-on-four-defence-affiliated-facilities-by-pakistan-based-groups-thwarted/article69506321.ece>

4. “Did Pak launch a cyber-attack on India’s electricity grid?”, *Financial Express*, 10 May 2025. <https://www.financialexpress.com/india-news/fact-check-did-pak-launch-a-cyber-attack-on-indias-electricity-grid/3839352/>
5. “It’s CHEAPFAKE! AI-generated video of EAM Jaishankar shared with false, fabricated, baseless claim”, PTI News, 10 May 2025. <https://www.ptinews.com/fact-detail/pti-fact-check-it-s-cheapfake-ai-generated-video-of-eam-jaishankar-shared-with-false-fabricated-baseless-claims-details-inside/2545264>
6. “Govt debunks claims of Indian female Air Force pilot Shivani Singh captured in Pakistan”, *The Times of India*, 12 May 2025. <https://timesofindia.indiatimes.com/india/fake-govt-debunks-claims-of-indian-female-air-force-pilot-shivani-singh-captured-in-pakistan/articleshowprint/121053492.cms>
7. “Meaning of Cyber Warfare”, Cambridge Dictionary. <https://dictionary.cambridge.org/dictionary/english/cyber-warfare>
8. F. Michael, “What do we know about cyber operations during militarized crises?”, Atlantic Council, 31 January 2022. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-do-we-know-about-cyber-operations-during-militarized-crises/>
9. “Pakistani hacker group claims to have breached Indian defence institution”, SATP, 06 May 2025. <https://www.satp.org/terrorism-update/pakistani-hacker-group-claims-to-have-breached-indian-defence-institutions>
10. “APT Profile Transparent Tribe aka Apt36”, CYFIRMA, 15 May 2025. <https://www.cyfirma.com/research/apt-profile-transparent-tribe-aka-apt36/>
11. “Cyber Attacks Rise as Tension Mounts Across India Pakistan Border Post Terrorist Attack”, Cyber Proof, 14 May 2025. <https://www.cyberproof.com/blog/cyber-attacks-rise-as-tension-mounts-across-india-pakistan-border-post-terrorist-attack/>
12. Dr Sameer Patil, “Operation Sindoor and India-Pakistan’s Escalated Rivalry in Cyberspace”, RUSI 20 June 2025. [Operation Sindoor and India-Pakistan’s Escalated Rivalry in Cyberspace | Royal United Services Institute](https://rusi.org/operation-sindoor-and-india-pakistan-s-escalated-rivalry-in-cyberspace)
13. “Essential Measures for MSMEs for Safeguarding Business Operations against Cyber Security Threats”, CERT-IN, 10 May 2025. [Advisories](https://cert.in/Advisories)
14. Pihu Yadav, “Inside the misinformation tsunami around India-Pakistan cyber threats”, CNBC, 12 May 2025. <https://www.cnbc18.com/technology/explainer-dance-of-the-hillary-fake-viral-message-india-pakistan-cyber-conflict-19603297.htm>
15. [PIB Fact Check \(@PIBFactCheck\) / X](https://twitter.com/PIBFactCheck), Government of India.
16. “Over 8,000 X accounts blocked in India; The Wire says will challenge site blocking”, *The Hindu*, 09 May 2025. <https://www.thehindu.com/news/national/x-says-it-blocked-8000-accounts-in-india-after-govts-executive-orders/article69554836.ece>
17. “Terror groups using digital platforms to promote ‘jihad’, says EFSAS researcher”, ANI, 22 June 2025. <https://www.aninews.in/news/world/europe/terror-groups-using-digital-platforms-to-promote-jihad-says-efsas-researcher20200622162532/>