MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Digital War: Pakistan's Cyber Activity Against India

Cherian Samuel and Rohit Kumar Sharma

May 16, 2025

Summary

Malicious actors were active as soon as reports of the Pahalgam attack began to surface, with a noticeable increase in their activities in the following days. Threat actors created fake domains that mirrored legitimate services, which were then used to deploy malware targeting the Indian government and defence personnel. Social media platforms were flooded with misinformation in a deliberate attempt to undermine public trust.

On 7 May 2025, exercising its "right to respond", Indian armed forces launched Operation Sindoor, under which they carried out precision strikes to destroy a network of terror camps in Pakistan and Pakistan-Occupied Kashmir. [1] The operation was undertaken in the wake of a terror attack in Pahalgam in which 26 tourists were murdered in cold blood. Defence Minister Rajnath Singh stated that the Indian armed forces carried out a focused, measured and non-escalatory response, intended to "break the morale" of the terrorists operating inside Pakistan.

Pakistani-affiliated hacker groups conducted a range of cyber attacks against Indian targets, even though none of them created any significant disruption. These attempts were first noticed following the Pahalgam attack and even before the escalation of the conflict, when websites associated with the armed forces were subjected to web defacement and online disruptions. Despite the fact that these intrusions were successfully thwarted by relevant agencies, the uptick in cyber attacks reflects a pattern seen in hot zones in Europe and West Asia.

Table 1. Cyber Operations against India following Pahalgam Attack

Incidents/Operations	**Type of attack**	**Response**
Cyber attacks on the websites of the Army Public Schools in Srinagar and Ranikhet	Web defacement Distributed denial-of-service (DDoS)	Swiftly rectified by web managers
Cyber incident targeting the Army welfare housing organisation database	Attempted network breach	Affected sites isolated and restored; no impact on classified network[2]
Incident targeting the Indian Air Force Placement Organisation Portal	Attempted network breach	No breach in classified network[3]
Incident targeting Rajasthan's Education Department	Webpage defacement with inflammatory messages	Adequate measures were undertaken, and no reports of sensitive data leaks were received.[4]

[1] "**India Exercised 'Right to Respond' through Operation Sindoor: Rajnath Singh**", *Hindustan Times*, 7 May 2025

[2] Vishnu Som, "**Pak-Based Hackers Target Army Public Schools, Other Indian Sites**", *NDTV*, 29 April 2025.

[3] Mayank Singh, "**Pakistan-based Hackers Target Armed Forces' Websites, India Foils Repeated Attempts**", *The New Indian Express*, 29 April 2025.

[4] Rajesh Asnani, "**Rajasthan Education Department Website Hacked; Message from 'Pakistan Cyber Force' Displayed**", *The New Indian Express,* 29 April 2025.

Scores of fake news regarding Indian armed forces operations, as well as the fake claim about 70 per cent of India's power grid hit by Pakistan	Part of the broader influence operations	Real-time updates by Press Information Bureau (PIB) fact-check to counter fake news.
APT36 attempting to target the Indian government and defence personnel.	Credential phishing, deployment of malicious payloads. The group has also created a network of spoofed domains to support its operations.	Threat intelligence firms tracking; no evidence yet of any breach.
News around "Dance of the Hillary Virus"	Data-stealing Trojan	Advisory and alert issued by relevant agencies.

Source: Media reports.

An early description of cyber-terrorism defines it as

> premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents....[5]

Government computer networks, financial networks, power plants, etc., are all possible targets as terrorists may identify these as the most appropriate features to corrupt or disarm in order to cause havoc. Manipulation of systems via software with secret "back doors", theft of classified files, erasing data, re-writing web pages, introducing viruses, etc., are just a few examples of how terrorism can penetrate secure systems.[6]

Besides the three conventional domains of warfare—land, air and sea—modern conflicts are also being waged in the cyber realm. There are abundant examples of state-backed and independent hackers on both sides of the Russia–Ukraine conflict who have been mobilised to impose costs on their adversaries through cyber attacks. Similarly, there was a sharp increase in the number of cyber incidents during the initial phase of the Israel–Hamas conflict. These cyber operations have so far fallen short of causing any major or significant impact. However, underestimating the significance of such operations based only on outcomes would be a strategic mistake.

[5] Kevin Curran, Kevin Concannon and Sean McKeever, "Cyber Terrorism Attacks", in Lech Janczewski and Andrew Colarik (eds), Cyber Warfare and Cyber Terrorism, IGI Global, Hershey, PA, 2007, pp. 1–6.

[6] Ibid

Scholars have long debated the role of cyber operations in managing escalation during a militarised crisis.[7] Strong doubts have been expressed about the role of cyber operations in crisis escalation, and the possibility of malicious behaviour in cyberspace leading to an armed conflict.[8] Instead, it is argued that cyber operations can be seen as a valuable way of projecting power, without indulging in armed conflicts.[9] Moreover, cyber operations "by their very nature are designed to avoid war".[10] There is also a view that cyber operations could serve as de-escalatory offramps in the crisis. Given the nature of cyberspace, it is argued that prudence needs to be practised when considering cyber operations, as it may lead to inadvertent escalation.[11]

Pakistan's Cyber Strategy

Pakistani aggression in the cyber realm can be categorised as Advanced Persistent Threat (APT) and hacker group activity, misinformation through social media platforms, and online activities by terror outfits. Pakistan-based APT groups actively targeted Indian infrastructure, conducting somewhat sophisticated and sustained operations against India's interests. For instance, the APT actor, APT36 or Transparent Tribe, a threat group attributed to Pakistan, has been active since 2013,[12] and has primarily targeted Indian defence, government and diplomatic entities.

APT36 is known for its reliance on Crimson RAT, a remote access trojan used for data exfiltration and espionage. It frequently mimics Indian government websites to distribute malware. Following the Pahalgam attack, APT36 launched a cyber attack campaign spoofing India's Ministry of Defence and "Pahalgam Terror Attack" themed documents to distribute malware, which could eventually be put to use to conduct information operations and espionage operations.[13]

Another Pakistan-based APT actor, Sidecopy, has also been active, sending out phishing emails impersonating official entities and delivering malware through fake domains mimicking legitimate services. During the conflict, Indian agencies

[7] Michael P. Fischerkeller, "**What Do We Know about Cyber Operations during Militarized Crises?**", Atlantic Council, 31 January 2022.

[8] Erica D. Lonergan, "**The Cyber-Escalation Fallacy**", *Foreign Affairs*, 15 April 2022.

[9] Ibid.

[10] Ibid

[11] Michael P. Fischerkeller, "**What Do We Know about Cyber Operations during Militarized Crises?**", no. 7.

[12] Alessandro Mascellino, "**Pakistan-Aligned Hackers Disrupt Indian Education Sector**", *Inforsecurity Magazine*, 13 April 2023.

[13] Rhishav Kanjilal, "**Advisory: Pahalgam Attack Themed Decoys Used by APT36 to Target the Indian Government**", *Seqrite*, 30 April 2025.

identified seven APT groups operating against India that were also responsible for over 15 lakh cyber attacks.[14] Most of these attacks reportedly originated from Pakistan, Bangladesh and the West Asian region. However, these groups are not technically as advanced as Chinese APTs, which leverage zero-day exploits and conduct supply-chain attacks.

These activities have been flagged by various government agencies, and advisories have been issued.[15] India has undertaken anticipatory measures to secure its critical infrastructure and sensitive assets, including energy, defence manufacturing, telecommunications and transport.[16] The Department of Telecommunications (DoT) has been evaluating measures to enhance infrastructure. At the same time, the Indian Computer Emergency Response Team (CERT-In) has issued advisories pertaining to risks to banks and financial institutions. An advisory outlining the essential measures that need to be undertaken to secure MSMEs[17] was issued on 10 May, followed by one for large industries. In the latter advisory, the agency reported a sharp rise in ransomware attacks, DDoS incidents, malware infections and web defacements.[18]

Hacker group activity was much less consequential, and was largely found to be exaggerated. Such claims were largely disseminated through social media with screenshots of apparently successful hacks. Upon examination, most of these were found to be repackaging of earlier inconsequential breaches or databases without sensitive information. Many of these groups also claimed to be based in other countries.[19]

Table 2. APT and Hacker Group Claims[20]

Groups’ names	Claims	Actual impact
SYLHET GANG-SG & DieNet	Exfiltration of around 247 GB of data from India’s National Informatics Centre (NIC)	Claims are largely unsubstantiated based on evidence provided.

[14] Mukesh Ranjan, “**15L Cyber Attacks on Key Locations by Pakistan Hackers**”, *The New Indian Express*, 14 May 2025.

[15] “**As Pakistani Hacker Group APT36 Targets Indian Systems, Chandigarh Police Issue Advisory**”, *The Indian Express*, 10 May 2025.

[16] “**Govt Ramps Up Cyber Vigilance on Critical Infrastructure after Operation Sindoor**”, *Money Control*, 7 May 2025.

[17] “**Essential Measures for MSMEs for Safeguarding Business Operations against Cyber Security Threats**”, CERT-IN, 10 May 2025.

[18] Ibid.

[19] Himanshu Lohchab, “**Border Fire Draws in Digital War, Tourists Looking for Quick Bucks**”, *Economic Times*, 14 May 2025.

[20] Pagilla Manohar Reddy, “**Brief Disruptions, Bold Claims: The Tactical Reality Behind the India-Pakistan Hacktivist Surge**”, *CloudSEK*, 11 May 2025.

Team Azrael-Angel of Death	Alleged breach of the Election Commission of India	No breach reported lately. The data released was leaked initially in 2023.
	Compromising and leaking data pertaining to Indian Army personnel and other agencies.	Data appears to be fabricated, not representing a legitimate compromise.
KAL EGY 319	Large-scale defacement operation targeting Indian educational and medical websites	Minimal impact; claims largely overblown
Coalition of groups including Lực Lượng Đặc Biệt Quân Đội Điện Tử, Vulture, and GARUDA ERROR SYSTEM	DDoS attacks against Indian government websites, including the PMO.	Websites are fully operational, no significant impact noticed.
SYLHET GANG-SG	Unauthorised access to records from the High Court	No massive breach reported. However the leak did expose some password hashes.
Vulture & the Electronic Army Special Forces	DDoS attack against CERT-In and the National Testing Agency (NTA).	No evidence of operational disruption; claim unfounded.

Source: CloudSEK

Nonetheless, they provided grist to disinformation campaigns at a time when uncertainty about the crisis was widespread. The aim was to spread deceptive, misleading, or biased information, usually through troll accounts, automated bots and coordinated mass messaging on platforms such as Twitter, Facebook and WhatsApp.

A manual count shows that the Press Information Bureau (PIB) issued more than 60 fact-checks over five days to counter this tsunami of misinformation.[21] This included claims that an Indian Sukhoi Su-30MKI fighter jet had been shot down in Pakistan-Occupied Kashmir (POK) and that an Indian pilot was captured. According to the PIB, the photo being used to support the claim shows a Sukhoi jet that had crashed in Maharashtra in 2014.

[21] **PIB Factcheck**, Government of India.

These manipulated stories, false narratives, deepfakes, fake or misattributed imagery, and fabricated news stories were further amplified through the use of polarising hashtags. Even independent experts were sometimes taken in by this flood of misinformation, which left little time for authentication and sometimes unwittingly contributed to the further spread of the canards. The Ministry of Electronics and Information Technology issued orders to social media platform X to block 8,000 accounts.

Pakistan’s use of terrorists against India has not been limited to the conventional domain. Terror outfits such as Lashkar-e-Taiba (LeT) and Jaish-e-Mohammad have leveraged cyberspace extensively for recruitment, propaganda, communication, funding, planning and executing attacks.[22] Internet and social media platforms—including Facebook, Twitter, WhatsApp, Telegram and YouTube—have been effectively used to spread extremist ideology and to recruit followers.

Encrypted messaging apps and private social media channels are central for operational coordination and secure communication among group members. The LeT, for instance, has organised online and offline social media workshops to provide knowledge on exploiting online spaces to spread LeT ideology and objectives, and incite youngsters to engage in anti-India protests in the Kashmir Valley. The LeT has also used online gaming as a recruitment tool, providing links to a game titled “Age of Jihad” on one of its websites.[23]

The pause in hostilities notwithstanding, reports are pointing out that threat actors are still targeting Indian government websites.[24] The attack envelope is also expanding with reports of GPS spoofing, which typically involves manipulating GPS signals using software, and which, given its dual use, points to the increasing hybridisation of the battlefield and its secondary effect as an attack on critical infrastructure in use by millions.[25]

Conclusion

The ongoing cyberattacks targeting Indian infrastructure suggest growing reliance on cyber operations before, during, and after the cessation of military hostilities. Malicious actors were active as soon as reports of the Pahalgam attack surfaced, with

[22] Munish Sharma, **“Lashkar-e-Cyber of Hafiz Saeed”**, Commentary, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), 21 March 2016.

[23] **“Social Media Strategies and Online Narratives of Terrorist Organizations; Case studies of Al-Qaeda, ISIS, Taliban and Lashkar-e-Taiba”**, European Foundation for South Asian Studies, 2020.

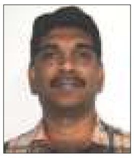
[24] **“Pakistani Hackers Attacked 1.5 million-plus Indian Websites after Operation Sindoor: Failure Rate, Names of 7 Pakistani Hacker Groups; Techniques Used and More”**, *The Times of India*, 13 May 2025.

[25] Ibid.

a noticeable increase in their activities in the following days. Existing threat actors like APT36 created fake domains that mirrored legitimate services, which were used to deploy malware targeting the Indian government and defence personnel. Social media platforms were flooded with misinformation in a deliberate attempt to undermine public trust in Indian operations.

The Indian government responded swiftly, successfully thwarting many of the attacks in time. Official Indian handles on social media platforms like X proved highly effective in identifying fake news and played a key role in identifying and taking down the accounts responsible. That said, tactics such as phishing emails, infected mobile apps, spyware, and embedding hidden malware on websites to gain unauthorised access to sensitive information can only be countered through continuous vigilance and strict digital hygiene practices.

About the Author



Dr. Cherian Samuel is Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses