CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 09/2025

20 May 2025

Cyber Warfare: Dual Operational Fronts in Contemporary India-Pakistan Conflicts

Mrs Gowri Ramakrishnan
Research Associate, Centre for Air Power Studies

Source: Adobe Firefly

Keywords: Cyber warfare, Pahalgam Terror Attack, Cyberattack, Disinformation

Cyberattacks during war and even during peacetime have become the new normal in recent years. Cyberspace is considered as one of the five key distinctive environments of warfare along with land, air, maritime, and space environments. [1] The recent terrorist attack in Pahalgam, India triggered in a military response by Indian Armed forces against Pakistan (the terrorism backers and planners) with 'Operation Sindoor' in which nine major terror camps were destroyed with the onset of operations on May 07, 2025. Subsequently, the armed conflict between India and Pakistan continued till May 10, 2025, wherein Pakistan attacked both the Indian civil and military establishments, though India carried out strikes only on selected terrorist hubs and military facilities aiding terrorism with long-range precision weapons to avoid any harm to Pakistani civilians. [2]

Cyberspace operations:

During this armed conflict, the cyberattacks against India saw a significant rise. The live threat attack maps provided by organisations such as Kaspersky [3] and Radware [4] indicate that India consistently ranks among the top five most targeted countries during and following the period of conflict. The Indian Computer Emergency Response Team (CERT-In) detected a surge in cyber threats such as ransomware attacks, Distributed Denial of Service (DDoS) attacks, website defacements and malware infections for Indian industries and Micro, Small, and Medium Enterprise (MSMEs). [5] The Maharashtra police recorded more than 10 lakh cyberattacks after the Pahalgam attack highlighting a significant surge in cyber threats linked to the ibid geopolitical tensions. [6] Over 500 Indian government and private sector entities were targeted by hacktivist groups, underscoring the growing threat of ideologically motivated cyberattacks against national infrastructure.[7] The hacktivist groups targeted critical infrastructures using different types of cyberattacks, aiming to disrupt and degrade operational efficiency. Some reports suggest that multiple hacktivist groups were engaging in strategic coalition-building, unifying under a single alliance to coordinate and amplify cyber offensive operations against the targeted state.[8]

The DDoS attacks to slow down the server, website, or network by sending malicious traffic were reportedly carried out in both India and Pakistan. The report claims over 500% increase in cyberattacks in India and more than 700% increase in Pakistan. [9] The attackers used DDoS attacks such as NTP (Network Time Protocol) amplification, CLDAP (Connectionless Lightweight Directory Access Protocol) reflection, NetBIOS reflection and ACK_FLOOD to attack various public and private websites of India and Pakistan. [10] However, Maharashtra Cyber has attributed over 1.5 million cyberattacks on India's critical infrastructure, following the Pahalgam terror incident, to seven Advanced Persistent Threat (APT) groups, with only 150 breaches reported as successful. [1112]

The Pakistan based DDoS cyberattacks targeted Indian websites like critical infrastructure (powergrid.in), educational institutions (ncccnews.com), government services (uidai.gov.in, pib.gov.in, pmindia.gov.in, jkgad.nic.in, presidentofindia.gov.in, ns2.nic.in), defence services (mod.gov.in), telecommunication services (bsnl.co.in), Media services(tv9hindi.com). [1314] These attacks rendered websites inaccessible for an extended period, significantly disrupting the services provided by these respective organisations. Phishing attacks were observed wherein threat actors impersonated Indian government entities, distributing malicious PDF payloads disguised as official documents outlining government response measures.[15] Pakistan suffered DDoS attacks in public, private websites [16] and hacking of several twitter handles. [17] The Indian Cyber Force claimed responsibility for compromising of several Pakistan based webcams across Industrial zones, Private corporations, Government facilities, Police stations, Schools and Banks & ATMs, as well as breaching of government websites (iris.fbr.gov.pk), [18] Pakistan Stock Exchange portal and official Twitter accounts such as (Karachi Port). [19] DDoS attacks were launched against various Pakistan-based websites, including telecommunications services (*worldcall.net.pk*), educational institutions (*qau.edu.pk*), emergency services (*rescue.gov.pk*), and government portals such as the Ministry of Commerce (*commerce.gov.pk*). [20] The persistence of cyberattacks even after ceasefire agreements highlighted the enduring nature of cyber conflict, with continued attempts to disrupt and steal data in digital infrastructure.

In the wake of escalating India-Pakistan tensions, not only have cyberattacks surged against Indian infrastructure, but a parallel front has opened in the form of aggressive disinformation campaigns. Following India's precision strikes on terror camps in Pakistan and Pakistan-occupied Jammu and Kashmir under Operation Sindoor, Pakistan launched a sustained disinformation drive, falsely claiming to have inflicted significant damage on key Indian military assets, including the advanced S-400 air defence system and BrahMos missile bases. These claims, widely circulated on social media and amplified by pro-Pakistani accounts, alleged that the Pakistani Air Force's JF-17 jets had destroyed the S-400 system at the Adampur air base and damaged several other strategic locations. [21] Several disinformation campaigns, such as false allegations of destruction of Indian Air fields/bases such as Adampur, Nagrota, Bhatinda, Jaipur and Delhi [22] aimed to incite public panic and disrupt civil stability within India. Instances of disinformation were observed wherein the adversary's info warriors were circulating previously leaked data on dark web forums and fabricating old incidents of Indian Air Force flight crashes as newly obtained information with the intent of inciting panic and confusion.[2324]

India's Actions & Responses:

As a precautionary measure, Indian stock exchanges restricted access to their websites from foreign IP addresses to mitigate potential cyber threats.[25] The Indian Computer Emergency Response

Team (CERT-In) issued specific advisories, especially in the wake of increased cyberattacks, to enhance national cyber resilience. Following breaches of defence-related websites, cybersecurity experts implemented more robust protective measures,[26] while public and private organisations issued threat advisories strengthen overall cyber defence infrastructure.

To counter the disinformation campaign, the Press Information Bureau (PIB) actively issued regular fact-check reports, and government officials issued press releases supported by evidence and official explanations, aimed towards dispelling propaganda campaigns targeting India, and the fabricated stories about India attacking Afghanistan and Iran seeking to isolate India diplomatically and portray it as a regional aggressor. [27] Pakistan leveraged state-backed media and its allies like Turkey and China tried to amplify false claims. Turkish outlets (TRT World, Anadolu Agency) echoed unverified narratives, such as Indian airbase destruction, to sway global opinion.[28]

Conclusion:

The conflict marked a paradigm shift in warfare, where cyber operations and disinformation campaigns became force multipliers for conventional military actions. The strategic recommendations to mitigate future cyber risks, flowing from the lessons of these escalations, are to make a centralised framework that would enable real-time threat intelligence sharing and standardised protocols for critical infrastructure protection, to develop mandatory cyber hygiene protocols for MSMEs and industries. India should build deterrence-through-strength by showcasing offensive cyber capacities, as hinted by unofficial retaliatory breaches of Pakistani banks. [29] CERT-In can conduct drills nationwide to simulate multi-vector attacks to test resilience. Public-private alliance in sharing real time threat intelligence should be strengthened to facilitate timely detection, coordinated response, and comprehensive protection against evolving cyber threats targeting critical infrastructure. Pakistan's hybrid warfare strategy with cyberattacks and false narrative campaigns focusing on disruption and confusion should be countered by implementing sustained and periodic public awareness campaigns through education and critical information dissemination. India's success in limiting breaches to 150 out of 1.5 million attacks [30] highlights growing technical prowess but exposes systemic vulnerabilities in pre-emptive threat detection and interagency coordination. Moving forward, the line between physical and digital battlefields would blur further. India's priority should be to institutionalise cyber resilience.

***

NOTES:

[1] Colin S. Gray, *Airpower for Strategic Effect* (Alabama: Air University Press, 2012), p. 14

[2] Press Information Bureau, India, "Operation Sindoor: India's Strategic Clarity and Calculated Force," May 12, 2025, https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154448&ModuleId=3. Accessed on May 14, 2025.

[3] "Cyberthreat Live Map," *Kaspersky*, https://cybermap.kaspersky.com/. Accessed on May 14, 2025.

[4] "Live Cyber Threat Map | Radware," *Radware*, https://livethreatmap.radware.com/ . Accessed on May 14, 2025.

[5] "CERT-In Advisory CIAD-2025-0019," *CERT-In*, https://www.cert-in.org.in/. Accessed on May 14, 2025.

[6] "Over 10 lakh Cyber Attacks on Indian Systems after Pahalgam Terror Attack: Maharashtra Cyber," *The New Indian Express,* May 02, 2025, https://www.newindianexpress.com/nation/2025/May/02/over-10-lakh-cyber-attacks-on-indian-systems-after-pahalgam-terror-attack-maharashtra-cyber. Accessed on May 14, 2025.

[7] Abdul Nazeer MA, "500 Indian govt, pvt Entities Targeted by Hacktivist Groups," *The New Indian Express*, May 08, 2025, https://www.newindianexpress.com/states/kerala/2025/May/11/500-indian-govt-pvt-entities-targeted-by-hacktivist-groups. Accessed on May 14, 2025.

[8] Nate Nelson, "After Pahalgam Attack, Hacktivists Unite Under #OpIndia," *Dark Reading,* May 10, 2025, https://www.darkreading.com/cyberattacks-data-breaches/pahalgam-attack-hacktivists-unite-opindia. Accessed on May 15, 2025.

[9] "Two Battlegrounds: India-Pakistan Conflicts and DDoS Attacks," *NSFocus*, May 08, 2025, https://nsfocusglobal.com/two-battlegrounds-india-pakistan-conflicts-and-ddos-attacks/. Accessed on May 15, 2025.

[10] Ibid.

[11] "Pakistan-Allied Hackers Launched 15 Lakh Cyber Attacks on Indian Websites; Only 150 Successful," *Press Trust of India*, May 13, 2025, https://www.ptinews.com/story/national/Pakistan-allied-hackers-launched-15-lakh-cyber-attacks-on-Indian-websites;-only-150-successful=/2550835. Accessed on May 15, 2025.

[12] "Meet the 7 Pakistani Hacker Groups That Tried to Breach India—and Failed Miserably." *The 420.in,* May 13, 2025, https://the420.in/pakistan-cyber-attacks-on-india-failed-apt-groups-exposed/. Accessed on May 15, 2025.

[13]

[14] "Two Battlegrounds: India-Pakistan Conflicts and DDoS Attacks," - NSFOCUS, Inc., May 08, 2025, https://nsfocusglobal.com/two-battlegrounds-india-pakistan-conflicts-and-ddos-attacks/; "India-Pakistan Conflicts Escalating: Military Operations and DDoS Attacks Making Targeted Strikes," *NSFOCUS, Inc., ,*" May 13, 2025, https://nsfocusglobal.com/india-pakistan-conflicts-escalating-military-operations-and-ddos-attacks-making-targeted-strikes/. Accessed on May 16, 2025.

[15] Rhishav Kanjilal, "Advisory: Pahalgam Attack Themed Decoys used by APT36 to Target the Indian Government," *Seqrite,* April 30, 2025,https://www.seqrite.com/blog/advisory-pahalgam-attack-themed-decoys-used-by-apt36-to-target-the-indian-government/. Accessed on May 16, 2025.

[16] "Two Battlegrounds: India-Pakistan Conflicts and DDoS Attacks," *NSFOCUS,* May 08, 2025, https://nsfocusglobal.com/two-battlegrounds-india-pakistan-conflicts-and-ddos-attacks/. Accessed on May 15, 2025.

[17] "Pakistan Faces Suspected Cyberattacks as Several Social Handles Post Suspicious Information, Then Retract," *Business Today*, May 05, 2025, https://www.businesstoday.in/india/story/pakistan-faces-suspected-cyberattacks-as-several-social-handles-post-suspicious-information-then-retract-475539-2025-05-09. Accessed on May 15, 2025.

[18] Ibid.

[19] "Pakistan faces Suspected Cyberattacks as Several Social Handles Post Suspicious Information, then Retract," *Business Today*, May 05, 2025, https://www.businesstoday.in/india/story/pakistan-faces-suspected-cyberattacks-as-several-social-handles-post-suspicious-information-then-retract-475539-2025-05-09. Accessed on May 15, 2025.

[20] "Two Battlegrounds: India-Pakistan Conflicts and DDoS Attacks," *NSFOCUS,* May 08, 2025, https://nsfocusglobal.com/two-battlegrounds-india-pakistan-conflicts-and-ddos-attacks/. Accessed on May 15, 2025.

[21] Press Information Bureau, India, "Operation Sindoor Factcheck," https://www.pib.gov.in/factcheckupdates.aspx?lang=1&reg=3. Accessed on May 15, 2025.

[22] Ibid.

[23] Pagilla Manohar Reddy, "Brief Disruptions, Bold Claims: The Tactical Reality Behind the India-Pakistan Hacktivist Surge," *Cloud SEK*, May 11, 2025, https://www.cloudsek.com/blog/brief-disruptions-bold-claims-the-tactical-reality-behind-the-india-pakistan-hacktivist-surge. Accessed on May 16, 2025.

[24] "Breaking down Pak's Fake Narrative Factory: How it Colluded with "Allies" to Launch "Info War" against India," *Indian Defence Research Wing*, May 15, 2025, https://idrw.org/breaking-down-paks-fake-narrative-factory-how-it-colluded-with-allies-to-launch-info-war-against-india/. Accessed on May 16, 2025.

[25] Shivendra Kumar, "BSE, NSE Restrict Access to Websites for Overseas users: Reports," *The Economic Times,* May 07, 2025, https://economictimes.indiatimes.com/markets/stocks/news/bse-nse-restrict-access-to-websites-for-overseas-users-reports/articleshow/120955528.cms?from=mdr. Accessed on May 16, 2025.

[26] "Indian Army Tightens Cybersecurity after Defence-Linked Websites come under Attack," *The Economic Times*, May 05, 2025, https://economictimes.indiatimes.com/news/defence/indian-army-tightens-cybersecurity-after-defence-linked-websites-come-under-attack/articleshow/120903126.cms. Accessed on May 16, 2025.

[27] "Operation Sindoor, Pakistani Disinformation, Pak Claims, India Pakistan: Propaganda, Outright Lies: How Pak Is Ramping Up Misinformation Warfare," *NDTV,* May 10, 2025, https://www.ndtv.com/india-news/operation-sindoor-pakistani-disinformation-pak-claims-india-pakistan-propaganda-outright-lies-how-pak-is-ramping-up-misinformation-warfare-8379832. Accessed on May 16, 2025.

[28] "Breaking down Pak's fake Narrative Factory: How it Colluded with "Allies" to Launch "Info War" against India," *Indian Defence Research Wing*, May 15, 2025, https://idrw.org/breaking-down-paks-fake-narrative-factory-how-it-colluded-with-allies-to-launch-info-war-against-india/. Accessed on May 16, 2025.

[29] David Sehyeon Baek, "Cyber Warfare in the May 2025 India-Pakistan Conflict," May 14, 2025, https://www.linkedin.com/pulse/cyber-warfare-may-2025-india-pakistan-conflict-david-sehyeon-baek-ygjoc. Accessed on May 15, 2025.

[30] "Pakistan-Allied Hackers Launched 15 Lakh Cyber Attacks on Indian Websites; Only 150 Successful," *Press Trust of India*, May 13, 2025, https://www.ptinews.com/story/national/Pakistan-allied-hackers-launched-15-lakh-cyber-attacks-on-Indian-websites;-only-150-successful=/2550835. Accessed on May 15, 2025.