

CYBER-ENABLED SUB-CONVENTIONAL WARFARE AND INDIA-PAKISTAN STABILITY

By
Muhammad Hasnain Raza Khan
Intern
India Study Centre (ISC), ISSI
Email Address: isc@issi.org.pk

Edited by
Hafiz Usama Hameed

October 8, 2026

(Views expressed in the brief are those of the author, and do not represent those of ISSI)



Introduction

Conflict is a significant phenomenon that has drastically changed over time. One of the most prominent examples of this evolution is cyber-enabled operations, which can be used to gather intelligence, influence adversary opinions, and disrupt systems without engaging in traditional military conflict.¹ Cyber-enabled operations represent a field of grey-zone activity that can span beyond the threshold of conventional armed conflict to include activities such as intelligence collection, influence operations, and disruption of adversary systems.

Being in a decades-old strategic rivalry several crises leading to military clashes, India and Pakistan are lately in a face-off in cyber-enabled warfare. With the emergence of nuclear deterrence, large-scale conventional warfare has become less appealing, and grey zone competition defined as a competition beyond the threshold of conventional warfare but still within the nuclear realm, is growing more appealing.² Digital infrastructure is vital to the functioning of key sectors including electricity, telecommunications, banking, government, and other critical sectors, and as both countries come to rely on it more and more, cyberattacks on these systems can pose new threats to strategic stability.

¹ International Institute for Strategic Studies, *Cyber Capabilities and National Power*, IISS Strategic Dossier (London: IISS, 2024), <https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/>.

² Stimson Center, "Cyber Quicksand? Uncharted Risks and Escalatory Dynamics in a Future India-Pakistan Crisis," September 2, 2025, <https://www.stimson.org/2025/cyber-risks-and-escalatory-dynamics-future-india-pakistan-crisis/>.

Pathways to unintended escalation include attribution difficulties, state-non-state actor ambiguity, and the possibility of misperception.

The aim of this Issue Brief is to explore the impact of sub-conventional operations enabled by cyber networks on the strategic stability between the two countries and what policy measures can be taken to reduce these risks.

Cyber-Enabled Sub-Conventional Warfare

Emerged as a recent phenomenon, cyber-enabled sub-conventional warfare comprises the use of digital means to achieve strategic goals other than by employing conventional military force.³ These activities are of strategic importance because of several characteristics. The state-non-state dichotomy is not always easy to determine; hacktivist groups and advanced persistent threats (APTs) that are likely state-sponsored may exist on the margins. Information operations can be damaging to perceptions without actually damaging the information itself. Information operations can affect perceptions and the narrative without physically destroying the information. Threats to critical infrastructure (energy, telecommunications, financial systems) raise the potential for impacts in the physical world when the digital world is impacted.⁴

Cyber Competition between India and Pakistan:

Historically recorded Indian and Pakistani cyber operations include espionage, information operations, and murky campaigns by state-sponsored actors.

Cyber Espionage: A cyber security firm named Sentinel One reported in July 2026 that some hacking groups linked to India targeted law enforcement agencies of Pakistan between February 2024 and April 2026.⁵ Balochistan police was affected by this hacking process; the hackers had also gained access to the complaint management system, where all the data of personal records and criminal case files were present.⁶ Khyber Pakhtunkhwa Police, Punjab Safe Cities Authority and Islamabad Police were also targeted. Khyber Pakhtunkhwa Police had reported increase in cyber activities during the Pakistan-India tensions, in which users login credentials were compromised. The Indian authorities

³ Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

⁴ International Institute for Strategic Studies, *Cyber Capabilities and National Power*.

⁵ Reuters, "China, India-Linked Hacking Groups Targeted Pakistani Law Enforcement, Report Says," July 9, 2026, <https://www.reuters.com/world/china/china-india-linked-hacking-groups-targeted-pakistani-law-enforcement-report-says-2026-07-09/>.

⁶ SentinelLABS, "China, India-Linked Hacking Groups Targeted Pakistani Law Enforcement," July 9, 2026, <https://www.sentinelone.com/labs/one-target-china-india-espionage-converge-on-pakistani-law-enforcement/>.

did not respond to the questions raised about these activities.⁷ This case demonstrates the way cyber espionage enables intelligence gathering without conventional confrontation. Meanwhile, the absence of an official response from the affected governments contributes to the uncertainty regarding attribution.

State-Non-State ambiguity: Advanced Persistent Threat 36 (APT 36) (Transparent Tribe) is a group linked with Pakistan since at least 2013.⁸ It was documented by cybersecurity researchers that APT36 is involved in targeting the Indian government and defense entities.⁹ In a cyber attack campaign the Indian System known as BOSS(Bharat Operating System Solutions) Linux Distribution has been targeted by this group through phishing emails delivering malicious desktop files.¹⁰ The Indian Government has supported this system where DeskRAT tool is used to ensure a remote access. The advanced espionage demonstrates the growing cyber capabilities from the group's evolution to website defacement.¹¹ Moreover, the Indian entities under gas, oil, railway and external affairs ministries were also targeted by a side copy group accessed as a sub cluster of APT 36.¹² These groups work independently or allegedly under state patronage; therefore, it remains uncertain whether to hold the adversary government responsible or not.

Information Operations: In 2020, EU DisinfoLab exposed a network named "Indian Chronicles". The investigation found a large group of sites and groups, with many of them running for years. Investigators said it was meant to weaken Pakistan's image abroad. They also said it could sway how people viewed Pakistan inside European and other global institutions.

This case highlighted the importance of how information warfare works beyond the social media posts and how it includes the media platforms and online websites to collectively amplify the narratives. It

⁷ Reuters, "China, India-Linked Hacking Groups.

⁸ CloudSEK, "Investigation Report: APT36 Malware Campaign Using Desktop Entry Files and Google Drive Payload Delivery," December 12, 2025, <https://www.cloudsek.com/blog/investigation-report-apt36-malware-campaign-using-desktop-entry-files-and-google-drive-payload-delivery>.

⁹ CloudSEK, "Investigation Report: APT36 Malware Campaign.

¹⁰ Infosecurity Magazine, "Pakistani-Linked Hacker Group Targets Indian Government," October 23, 2025, <https://www.infosecurity-magazine.com/news/pakistani-hacker-group-targets/>

¹¹ The Hacker News, "Pakistan-Linked Hackers Expand Targets in India with CurlBack RAT and Spark RAT," April 14, 2025, <https://thehackernews.com/2025/04/pakistan-linked-hackers-expand-targets.html>.

¹² Pakistan Today, "Tara Claims India-Linked Digital Propaganda Network Targeted Pakistan through Online Drive," July 27, 2026, <https://www.pakistantoday.com.pk/2026/07/27/tara-claims-india-linked-digital-propaganda-network-targeted-pakistan-through-online-drive>.

also illustrated the challenges of differentiating the information activities between the states and private actors.¹³

Cyber Activities and Infrastructure Risks in India-Pakistan:

The cyber element of India-Pakistani rivalry was more prominently featured in May 2025 military standoff, where there were reports of cyber operations going along with the armed engagements. In the Operation Sindoor, Indian security forces have detected an increase in cyberattacks against various government departments and sensitive industries, including distributed denial-of-service (DDoS) attacks, data breaches, and malware attacks. Indian officials also said that during the crisis period the power sector was targeted by cyber-attacks, which were said to have been thwarted and the system has continued to operate.¹⁴ The developments prove how vulnerable the country's critical infrastructure can be in times of high tension between India and Pakistan. Disruption of power, telecommunication, and other critical infrastructure can also impact other operational issues, including uncertainty about who is responsible for the cyber incident and the perception of what the adversary will do next. It could prove to be a problem in future India-Pakistan conflicts when it comes to decision making, and can further escalate the possibility of retaliation. Hence, there is a need to safeguard critical infrastructure and to have mechanisms in place for communication between the two nuclear-armed states in the event of a cyber incident.¹⁵

Strategic Stability Implications

The cyber-enabled activities have unique risks for India-Pakistan strategic stability. Even if sophisticated cyber operations have not historically been a dominant feature of major South Asian crises like the Kargil crisis or the 2019 Pulwama-Balakot crisis; cyber activities are giving way to some uncertainty, trust deficit, and change in decision-making thresholds that are low intensity, but

¹³ Gary Machado et al., *Indian Chronicles: Deep Dive into a 15-Year Operation Targeting the EU and UN to Serve Indian Interests* (Brussels: EU DisinfoLab, December 9, 2020), <https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/>.

¹⁴ Sameer Patil, "Operation Sindoor and India-Pakistan's Escalated Rivalry in Cyberspace," Royal United Services Institute, June 20, 2025, <https://www.rusi.org/explore-our-research/publications/commentary/operation-sindoor-and-india-pakistans-escalated-rivalry-cyberspace>.

¹⁵ Nazir Masoodi, "2 Lakh Cyber Attacks on India's Power System During Op Sindoor: Minister," NDTV, June 12, 2025, <https://www.ndtv.com/india-news/2-lakh-cyber-attacks-on-indias-power-system-during-operation-sindoor-minister-8653484>

persistent over time.¹⁶ It becomes challenging to make decisions when determining the perpetrators. Decisions about who is responsible and what is their intent may be unclear when a cyber incident happens. The lack of a clear distinction between state and non-state entities raises questions concerning the responsibilities of a state for operations carried out by potentially affiliated entities. Standalone cyber-attacks may not necessarily lead to escalation of military operations; however, lack of doctrine for the integration of cyber operations may create uncertainty and misperception which may increase the likelihood of military escalation.

Policy Challenges Faced by Pakistan

Pakistan faces a number of challenges in ensuring cyber security. Major threats to cyber security include the poor quality and inadequacy of resources because they lead to challenges in coordinated responses to attacks.¹⁷ The difference between the activities of criminals, hacktivists and state actors makes threat assessment challenging. Lacking any specific crisis-management systems for cyber, risk reduction is further complicated.

Policy Recommendations

In the first place, Pakistan must adopt a holistic strategy aimed at building cyber resilience, especially against the critical infrastructure and important digital systems. The National Cyber Security Policy 2021 lays down the security standards and processes to be followed for the security of National Critical Information Infrastructure.¹⁸

Secondly, the authorities need to improve the attribution capacity on technical, intelligence and inter-agency capacity development. Better attribution will minimize uncertainty and help to inform calibrated action.

Thirdly, it is equally critical to strengthen institutional coordination, with clear sequences and information sharing to ensure that coherent cyber security policy is put into effect. The policy creates a Cyber Governance Policy Committee to be responsible for national cyber security issues.¹⁹

¹⁶ Stimson Center, "Cyber Quicksand? Uncharted Risks and Escalatory Dynamics in a Future India-Pakistan Crisis," September 2, 2025, <https://www.stimson.org/2025/cyber-risks-and-escalatory-dynamics-future-india-pakistan-crisis/>.

¹⁷ Pakistan, Ministry of Information Technology and Telecommunication, "National Cyber Security Policy 2021," 3–5, <https://moitt.gov.pk/SiteImage/Policies/NationPolicy%202021%20Final.pdf>.

¹⁸ Pakistan, Ministry of Information Technology and Telecommunication, "National Cyber Security Policy 2021," 7.

¹⁹ Pakistan, Ministry of Information Technology and Telecommunication, "National Cyber Security Policy 2021," 6.

Fourthly, there is a need to initiate discussion with India over cyber-specific crisis communication processes in order to minimize misperception in times of crisis. The lack of historical precedents surrounding cyber operations in South Asia means there is uncertainty that may be resolved through communication, as Stimson Center has proposed.

Finally, Pakistan should also explore confidence-building measures in cyber domain— practical arrangements related to critical infrastructure protection, notification of cyber incidents, or responsible state conduct. These measures should be undertaken with great care alongside the wider strategic dialogue.²⁰

Conclusion

Sub-conventional warfare in India-Pakistan strategic competition adds a new twist with the help of cyber. They offer other ways to achieve objectives that are below the conventional threshold and create uncertainty, misperception, and escalation risks. Strategic stability is complicated by attribution problems, state-non-state ambiguity as well as possible miscalculation. While it is impractical to completely remove cyber competition, the goal is not to eliminate it but to lessen uncertainty, improve resilience and attribution, and establish hindrances to cyber incidents “from becoming catalysts for further escalation.” In a world where deterrence has worked to stop traditional war yet competition has persisted in other fields of warfare, dealing with the threats of sub-conventional warfare enabled by cyber technology should be a top priority for Pakistan's national security establishment.

²⁰ Stimson Center, "Cyber Quicksand?"