



| Flash |

Threat Actors Join Targeting of India and Pakistan

F-2025-05-08a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Geopolitical, Deep and Dark Web

May 8, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 7:00 AM (EDT) on May 8, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Actors Join Targeting of India and Pakistan

| Key Findings

- While unlikely, there is a possibility that India's retaliatory attack for the Pahalgam attack and Pakistan's looming retaliation will lead to all-out war.
- India in particular is utilizing unprecedented non-military options to retaliate economically and via cyberattacks. An uptick in trade tensions and cyberattacks is very likely over the long term.
- ZeroFox has observed cyber threat actors on both sides targeting cyber infrastructure related to the defense sector.

| Background

On May 7, 2025, India struck at least nine sites in Pakistan in retaliation for an April 22 terrorist attack that killed over two dozen Indian civilians in the disputed territory of Kashmir. India blames Pakistan for supporting the militants who conducted the attack, which Pakistan denies. Indian authorities claimed the targeted sites were used to train and house militia groups, while Pakistani officials claimed they were predominantly

civilian areas and included several mosques.¹ At least 26 deaths have been reported in Pakistan so far as a result of the strikes.²

| Details

Pakistan has vowed a proportionate response to the strikes. Pakistani and Indian border guards exchanged heavy gun and artillery fire in the immediate aftermath of the attack; reportedly, at least 10 Indian civilians were killed in the cross-border shelling. Pakistan also claimed to have shot down five Indian warplanes and taken a number of Indian soldiers prisoner, though this was not immediately verified; Indian authorities later confirmed the loss of three warplanes without elaborating.³ Authorities in Pakistan have vowed a more significant response at an indeterminate point in the future.

- Pakistan's ability to shoot down Indian aircraft, including drones, demonstrates its significant defense capabilities and is likely a restraint on India.
- Pakistan's response will likely focus on Indian military targets, risking escalation.

Historically, there have been cross-border skirmishes between the nuclear-armed neighbors, although recent incidents have eventually de-escalated. However, several factors differentiate these strikes from those that have come before. First, India's targets included sites in Pakistan proper, as opposed to previous operations wherein Indian forces only struck sites in Pakistan-administered Kashmir, which India claims as its own.⁴

- India recently targeted sites in areas just north of the capital of Islamabad, as well as just outside the major southern city of Lahore. This is a significant escalation, as areas targeted during previous conflicts were located in remote parts of Pakistan and Kashmir.

¹

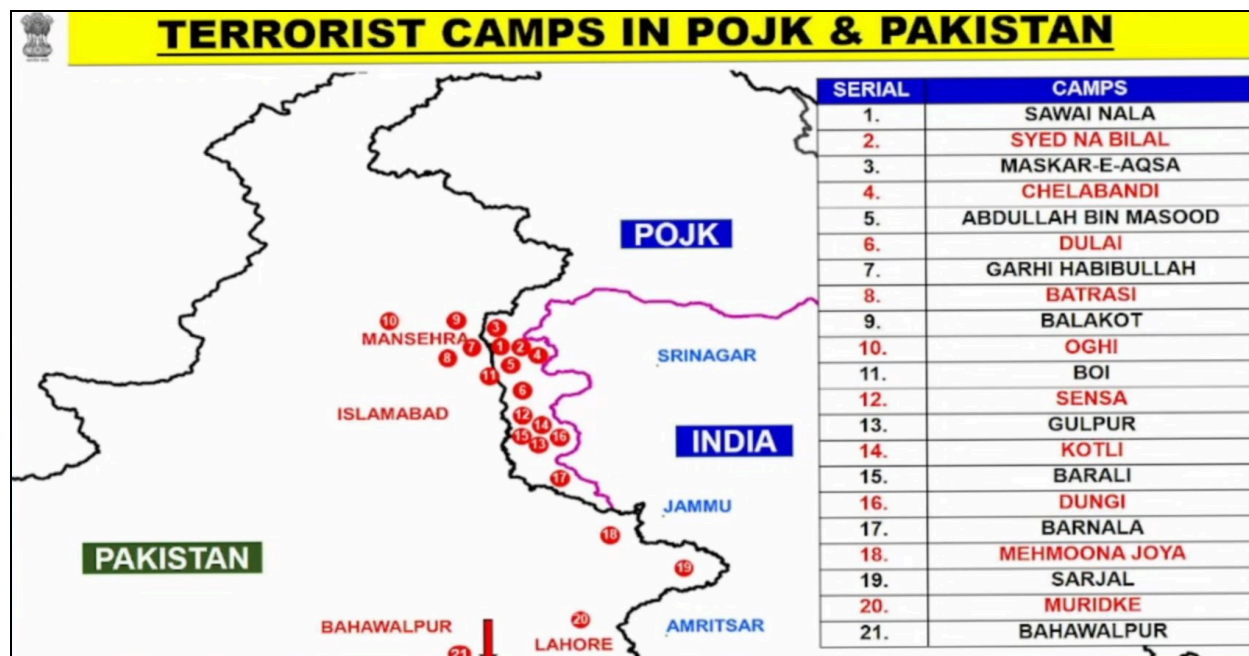
[hXXps://www.qcnews\[.\]com/news/national-news/ap-the-latest-india-fires-missiles-across-the-border-with-pakistan-killing-at-least-officials-say/](https://www.qcnews.com/news/national-news/ap-the-latest-india-fires-missiles-across-the-border-with-pakistan-killing-at-least-officials-say/)

² [hXXps://apnews\[.\]com/live/india-pakistan-attack-pahalgam-kashmir](https://apnews.com/live/india-pakistan-attack-pahalgam-kashmir)

³

[hXXps://www.reuters\[.\]com/world/asia-pacific/three-fighter-jets-crashed-indias-jammu-kashmir-local-govt-sources-say-2025-05-07/](https://www.reuters.com/world/asia-pacific/three-fighter-jets-crashed-indias-jammu-kashmir-local-govt-sources-say-2025-05-07/)

⁴ [hXXps://www.nytimes\[.\]com/2025/05/06/world/asia/india-pakistan-attacks.html](https://www.nytimes.com/2025/05/06/world/asia/india-pakistan-attacks.html)



Recent Indian targeting locations, including Lahore

Source:

[hXXps://english.gujaratsamachar\[.\]com/news/national/in-just-25-minutes-indias-operation-sin-door-strikes-9-terror-camps-in-pak-kills-70-terrorists](https://english.gujaratsamachar[.]com/news/national/in-just-25-minutes-indias-operation-sin-door-strikes-9-terror-camps-in-pak-kills-70-terrorists)

Second, India's recent threats to cut off Pakistan's water supply by unilaterally suspending the Indus Water Treaty are likely to be viewed by Pakistan as an existential threat, increasing the risk of a more forceful response from Pakistan's military.⁵

- India has also cut off all trade with Pakistan and is pressuring other trading partners to do so as well.⁶ This suggests that India's long-term plan is to hurt the Pakistani economy, isolate it from trade, and take advantage of its water scarcity. Pakistan is likely to view escalating its military operations as key to thwarting these initiatives.

⁵

[hXXps://economictimes.indiatimes\[.\]com/news/india/indias-water-will-flow-only-in-india-vows-pm-modi-amid-tensions-with-pakistan-over-suspension-of-indus-waters-treaty/articleshow/120937628.cms](https://economictimes.indiatimes[.]com/news/india/indias-water-will-flow-only-in-india-vows-pm-modi-amid-tensions-with-pakistan-over-suspension-of-indus-waters-treaty/articleshow/120937628.cms)

⁶

[hXXps://economictimes.indiatimes\[.\]com/news/india/india-demands-adb-stop-funds-to-pakistan-as-fallout-of-pahalagam-terror-attack-deepens/articleshow/120899083.cms](https://economictimes.indiatimes[.]com/news/india/india-demands-adb-stop-funds-to-pakistan-as-fallout-of-pahalagam-terror-attack-deepens/articleshow/120899083.cms)

Third, Indian Prime Minister Narendra Modi has staked significant political capital on suppressing militant activity in Kashmir and now likely finds himself under significant pressure to show strength regarding the territorial dispute with Pakistan.

Finally, if Pakistan's claims of downing multiple Indian warplanes are confirmed, there is a roughly even chance India will escalate the conflict in future strikes. The loss of a single warplane in 2019 skirmishes was widely reported as a humiliation for India,⁷ making it likely that multiple losses in a single night incentivizes New Delhi to double down.

Despite these risks, both sides have made overtures to de-escalate the conflict. Indian authorities labeled the strikes as "focused, measured and non-escalatory", and the recent post "Justice is served" on the India military's X account implies that immediate operations are complete.^{8,9}

- Failing to take military action likely would have damaged Modi politically; however, after emphasizing that India's military response was the biggest in decades, he may be prepared to de-escalate the conflict if Pakistan does. India telegraphed its desire to respond before launching its attack as well, which likely gave Pakistan ample time to prepare.
- India's non-military responses thus far have arguably been more unprecedented. This suggests they are likely to continue versus military responses, which have historically not resolved the issue of anti-India militancy coming from Pakistan.

Pakistan's vow to respond at a later time, rather than immediately, may also be meant to keep the conflict relatively contained. Still, the risks of miscalculation remain high, and escalation into a broader regional conflict cannot be ruled out.

Cyber Threats Focus on Military and Government

In the lead-up to the May 7 military strikes, ZeroFox observed several notable examples of cyber threat actors targeting the defense sectors on both sides of the conflict. This contrasts with findings in the immediate aftermath of the Pahalgam attack, when ZeroFox observed a major uptick in social media users sharing incendiary posts and mis/disinformation, as well as hacktivists threatening retaliation on Telegram.¹⁰

⁷ [hXXps://www.nytimes\[.\]com/2019/03/03/world/asia/india-military-united-states-china.html](https://www.nytimes.com/2019/03/03/world/asia/india-military-united-states-china.html)

⁸ [hXXps://www.nbcnews\[.\]com/world/india/india-pakistan-jammu-kashmir-rcna205229](https://www.nbcnews.com/world/india/india-pakistan-jammu-kashmir-rcna205229)

⁹ [hXXps://x\[.\]com/adgpi/status/1919850036596199492](https://x.com/adgpi/status/1919850036596199492)

¹⁰ ZeroFox Intelligence Flash Report: India-Pakistan Tensions Likely to Escalate – April 29, 2025

On May 7, 2025, ZeroFox observed that threat actor group “Mr Hamza” posted a message on its Telegram channel using the hashtag #Op_India, claiming to have carried out a series of cyberattacks against Indian military targets in response to the recent air strikes. Following this, Mr Hamza also allegedly carried out a series of distributed denial-of-service (DDoS) attacks targeting the official websites of the Indian Army, Indian Navy, Indian Air Force, and the Minister of Defence.¹¹

On May 6, 2025, newly emerged pro-Pakistan threat actor group “DesertCr0ws” claimed to have leaked data associated with the “Government of Punjab, India” on its Telegram channel, [hXXps://t\[.\]me/desertcrows](https://t.me/desertcrows). The threat actor claims to have leaked private data associated with more than 250,000 Punjab government employees, including prominent chief ministers, judges, university professors, and doctors. The leaked data allegedly includes serial numbers, departments, organizations, usernames, names, designations, and phone numbers.¹²

On May 6, 2025, threat actor “xuii” advertised a data breach of the Pakistani defense sector on the predominantly Russian-language dark web forum Exploit. According to xuii, the breached data includes confidential files and future strategic plans related to the defense sectors of Pakistan, China, and Turkey covering the period from 2025 to 2035. The actor is charging USD 1,000 for the data breach and claims the documents included show Pakistan acquiring weaponized drone capabilities.¹³

- Pakistan said it has used Chinese jets and missiles to down Indian aircraft in the latest military operations, while Turkey is a well-known provider of drones across global conflict zones.¹⁴¹⁵

¹¹ ZeroFox Intelligence

¹² ZeroFox Intelligence

¹³ ZeroFox Intelligence

¹⁴

[hXXps://www.scmp\[.\]com/news/china/military/article/3309480/pakistan-claims-chinese-made-j-10c-fighter-jets-used-against-indias-air-force](https://www.scmp.com/news/china/military/article/3309480/pakistan-claims-chinese-made-j-10c-fighter-jets-used-against-indias-air-force)

¹⁵

[hXXps://www.forbes\[.\]com/sites/pauliddon/2025/04/06/turkeys-best-drones-are-being-shot-down-over-middle-east-and-africa/](https://www.forbes.com/sites/pauliddon/2025/04/06/turkeys-best-drones-are-being-shot-down-over-middle-east-and-africa/)

[Home](#) > [Commerce](#) > [Buying/Selling](#) > [\[Access\] - FTP, shells, root, sql-inj, DB, Servers](#) > [Selling Pakistan Defence Production Data Includes Confidential Files & Future strate...](#)



Selling Pakistan Defence Production Data Includes Confidential Files & Future strategic to China and Turkey 2025 Plans 2025

By xuii, 3 hours ago in [\[Access\] - FTP, shells, root, sql-inj, DB, Servers](#)

[Follow](#) 1

[Start new topic](#) [Reply to this topic](#)



xuii
kilobyte
●●

Paid registration

26 posts

Joined

03/29/22 (ID: 127987)

Activity

хакинг / hacking

Autogaran

1

Posted 3 hours ago

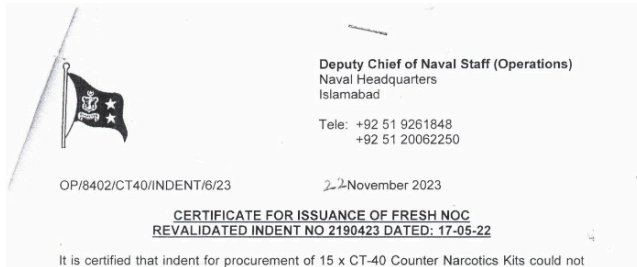
Hello,

The data we have includes information related to the Pakistan Navy as well as to Pakistan defence productions.. We have downloaded all the data, and we can also provide live access to it if needed.

The data also includes a strategic plan related to the defence sectors of Pakistan, China, and Turkey, covering the period from year 2025 to 2035.

price: 1000\$ forum garant accepted

see sample data



SWOT Analysis of Key Players & DP Institutions and Strategic Recommendations for Pakistan's Defense Production Industry

7. Pakistan's defense production industry has potential, but it faces structural challenges that hinder its growth and global competitiveness. This section provides a solid foundation for understanding the current state; however, improvements can be made by drawing comparisons from successful defense industries worldwide, such as Turkey, India, Ukraine, and China. Below is a SWOT Analysis of Pakistan Defence sector along with strategic recommendations.

a. SWOT Analysis of Pakistan's Defense Industry

(1) Strengths

- Established Public Sector Defense Institutions.
- Heavy Industries Taxila (HIT), Pakistan Ordnance Factories (POF), Pakistan Aeronautical Complex (PAC), and Karachi Shipyard & Engineering Works (KSEW) have strong capabilities in armored vehicles, ammunition, aircraft, and naval vessels.
- Competitive pricing due to lower labor costs.
- Proven Capability in Indigenous Production.
- JF-17 Thunder multirole fighter is exported to Nigeria, Myanmar, and Azerbaijan.
- HIT produces Al-Khalid tanks and armored vehicles that have export potential.

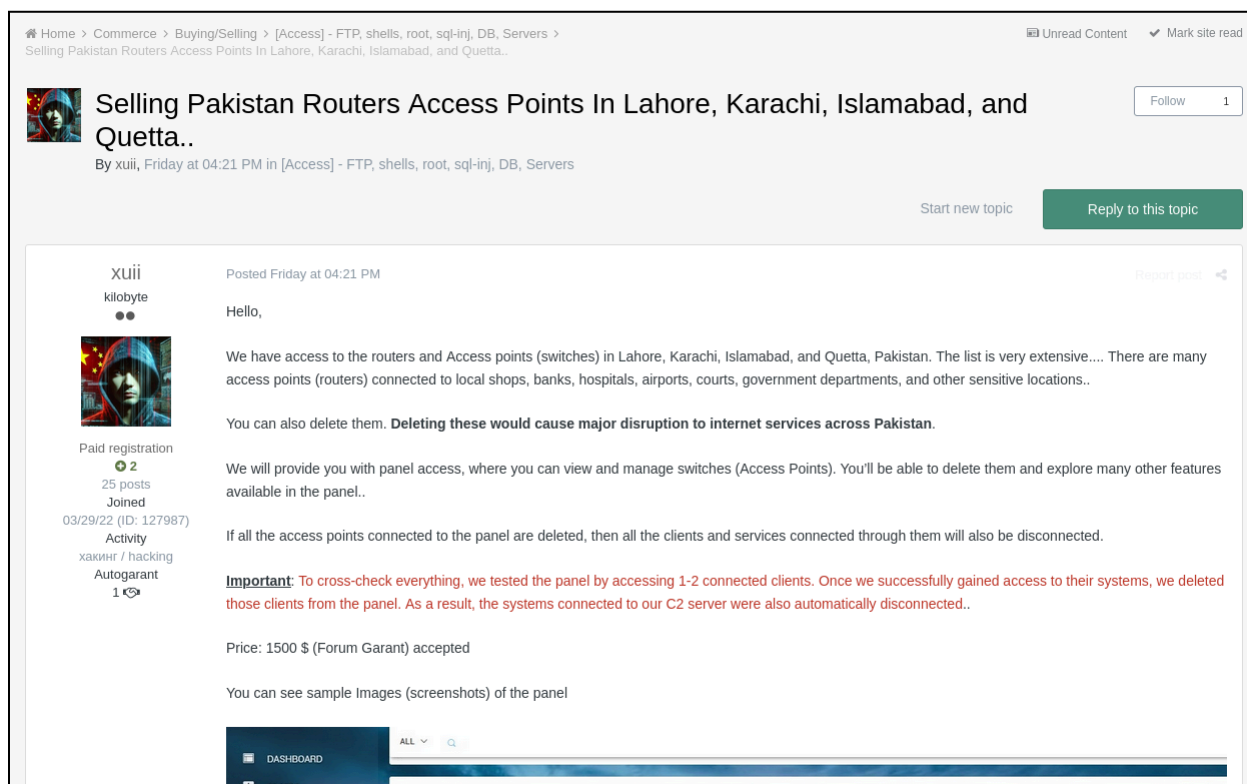
Data leaks pertaining to Pakistan defense agreements with China and Turkey

Source: ZeroFox Intelligence

© 2025 ZeroFox, Inc. All rights reserved.

6

On May 2, the same threat actor advertised web panel access with administrator rights to Pakistani network infrastructure. According to xuii, the infrastructure covers routers and access points to local shops, banks, hospitals, airports, courts, and government departments in the large Pakistani cities of Lahore, Karachi, Islamabad, and Quetta. The access was advertised for USD 1,500 and allegedly provides the ability to delete these access points.¹⁶



Threat actor advertisement of web panel access to Pakistani network infrastructure

Source: ZeroFox Intelligence

On April 29, xuii shared a scanned copy of a confidential letter from the Pakistani Prime Minister's Office. The content of the letter was about the hospitalization of the Prime Minister, and it was signed by the Principal Secretary to the Prime Minister.¹⁷

¹⁶ ZeroFox Intelligence

¹⁷ ZeroFox Intelligence

| Conclusion

India and Pakistan have fought three wars since their mutual independence in 1947, with the most recent occurring in 1971. Since then, they have managed to avoid full-blown military confrontations, despite coming close several times. There are incentives for both sides to de-escalate this time. India is engaged in negotiations for several important trade deals, including with the United States and the United Kingdom, that will likely open its historically protectionist economy. A full-blown war with Pakistan would very likely diminish the economic and trade appeal of working with one of the world's largest untapped trade markets. Pakistan is even more economically vulnerable and risks being cut off further in the event of war.

However, there are key domestic differences in this recent conflict. The April 22 attack, wherein gunmen specifically targeted Hindus, sparked domestic outrage in India, as Prime Minister Narendra Modi has spent years securitizing and promoting Kashmir as a tourism venue. For its part, Pakistan cannot risk looking weak just after recently subduing the powerful opposition bloc led by former Prime Minister Imran Khan.

In lieu of a full-blown conflict, both sides have other means to retaliate. India has led by suspending a key water treaty and severing bilateral trade agreements. Cyberattacks also appear to be a key form of alternative retaliation. For now, the cyber activity does not appear state-sponsored, but India in particular likely has the capabilities to target sensitive Pakistani infrastructure much in the same way it is conducting more precise strikes on areas it considers to be terrorist bases.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%