ARTICLES

Beyond Deniability: How the Shahzad Bhatti Network Could Be Reshaping Proxy Warfare

Author: Valluru Anvitha Reddy • **Published:** October 03, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Proxy warfare is evolving beyond traditional, permanent militant organisations towards flexible networks built around criminal links, digital recruitment and task-based operatives. Using the Shahzad Bhatti Network as a case study, this article examines how such networks can create a cycle of experimentation, learning and adaptation while remaining difficult for sponsors to control.

1. Introduction

States use proxy warfare to fight indirectly. By funding or equipping non-state actors, sponsors push their strategic interests without direct involvement. While this tactic is old, its mechanics are shifting.[1]

While deniability remains central by masking the conflict's source, proxies also reduce the military and political costs of direct confrontation while providing valuable local knowledge and networks. However, deniability may no longer be the sole driver for maintaining a proxy in the modern era.[2]

Historically, proxy warfare relied on structured militant groups with established leadership and long-term sponsor relationships, but these require heavy resources, are difficult to maintain, and are highly exposed to target states. Today, technological breakthroughs and the changing relationship between organised crime and terrorism create new possibilities. Modern proxy activity is shifting toward hybrid models, using criminal networks, online recruitment, and loosely connected operatives hired for specific tasks.[3]

Shahzad Bhatti, a Pakistani gangster linked by Indian authorities to ISI-backed terrorism, provides a clear example of this modern trend. The Shahzad Bhatti Network operates by blending organized crime with digital recruitment and terrorism. In 2026, Indian investigations revealed that the network was actively recruiting within India. Authorities also tied the group to logistics operations, weapons smuggling, and the early stages of planning targeted attacks.[4]

This case suggests that a proxy's value goes far beyond the physical violence it inflicts. We can view the proxy as a *"laboratory."* Every operation, even a failed one, triggers a reaction from the target state that provides crucial information to plan future operations. While the traditional view assumes a proxy merely attacks a target, this paper argues that the proxy also teaches the sponsor about the target's defence. This article analyses the SBN to explore how modern proxy warfare has become a continuous cycle of experimentation, learning, and adaptation.

2. The Evolution of Proxy Warfare

The traditional model of proxy warfare is straightforward: a state sponsor provides money, weapons, or intelligence, and the proxy carries out activities to serve the sponsor's interests, but scholars argue that this framework is too simple for contemporary conflicts, which rarely involve a neat, one-to-one relationship between a single state and a single group. Sponsors often interact with multiple entities, while proxies maintain their own agendas and alternative funding sources. Rather than remaining fixed, these relationships evolve over time, shifting from permanent organisations into fluid networks with varying degrees of connection to the sponsor.[5]

During the Cold War, proxies were usually identifiable political or ideological organisations. Today, digital communications, social media, and transnational networks have changed cross-border coordination greatly. Traditional militant groups still exist, but the pool of potential proxies has grown. Modern proxy warfare frequently blends militias, criminal networks, and loosely connected individuals. This makes operations highly networked and flexible, meaning a sponsor no longer needs to build a massive, all-in-one organisation when different niche actors can be used for specific functions.[6]

Proxy warfare works best as a long-term strategy that adapts rather than a rigid setup. While states can deploy basic proxy operations somewhat quickly, developing an advanced system involves learning and adaptation. Over repeated operations, a sponsor can gain experience in recruitment, cyber-coordination, logistics, and relationship management. If proxy warfare involves this kind of capacity building, individual operations become opportunities for experimentation too. This raises a critical question: what exactly is the sponsor learning, and how does that information shape the next operation?

3. Inside the Bhatti Network

Indian investigations show that Shahzad Bhatti was originally linked to cases of local violence and organised crime. By 2026, Indian agencies were tracking his alleged involvement in a much wider cross-border network tied directly to Pakistan's ISI.[7] This shift proves that the network did not start as a conventional, ideologically driven militant group, and reveals a completely different pathway into proxy warfare; one built on existing crime groups rather than established terrorist organizations.

Indian investigative reports show that the network used social media to recruit operatives inside India. The SBN bypassed traditional recruitment. Instead of pulling members into formal camps, it relied on fluid, task-based digital hiring. Recruits were approached online for minor jobs, like filming a police station or setting up a CCTV camera, before being pushed toward high-risk activities, weapons transport, and attack planning.[8] Under this, an operative does not need to be a deeply committed member of an organisation; they just need to be useful for a single job. That is a huge distinction from the traditional proxy model.

The SBN seems to combine three different elements: criminal networks that provide street-level contacts, local violence, funding pipelines, and an established underworld network; digital platforms like Instagram and Facebook that allow handlers to source and manage targets remotely without physical proximity; and terrorist/proxy operations that execute tasks like surveillance, logistics, weapons transport, and planned strikes.[9] So, instead of thinking of SBN as simply **"**a street gang" or "a terrorist organisation," it is more accurate to see it as a flexible network where different components handle different functions.

What sets SBN apart is how it links these disconnected actors without requiring permanent membership. The August crackdown gives some indication of the network's geographical spread: Indian authorities reported 253 people detained across 14 states, with more than 80 FIRs and 200+ arrests associated with the network. Recoveries reported by the government included IEDs, grenades bearing Pakistan Ordnance Factory markings, pistols, ammunition and CCTV equipment.[10]

When a sponsor hires random people for one-off attacks, is the goal just to cause damage, or is it to test the enemy's defences?

4. The Proxy as a Laboratory

Usually, we judge a proxy by its direct impact on the target: whether it carries out an attack, gathers intelligence, or creates political instability, but every proxy operation produces a secondary outcome that is easy to overlook: the target state's response. When a network operates, it triggers a response from the target state.[11] These responses reveal something about how the target state detects and responds to threats. So, a proxy operation always produces two outputs: a direct physical effect, and invaluable data about the target's security system. [10]

This article treats the proxy as a laboratory, which acts as a feedback loop rather than a rigid tool. Sponsors run real-world tests on recruitment, remote communication, and infiltration to see what holds up. Such learning does not require a formal experimental process; it can emerge through repeated operations.

Proxy warfare is usually treated as a one-directional process: the sponsor uses a proxy to attack a target, but if the proxy generates feedback, the process becomes circular. The target's response becomes information that can shape the next operation. [11] The process can be understood as a cycle: the network recruits an individual for a specific task; Indian authorities respond through countermeasures; and the network can then observe what went wrong and adjust future activity. Through repeated interactions, lessons may be learnt even without a formal training process.

Even a failed operation gives information about the target. It exposes how quickly local authorities detect suspicious behaviour, which surveillance tools are effective, and what vulnerabilities caused the plan to collapse. If a sponsor can observe these outcomes, failure itself becomes a source of information, creating a process of learning through failure.

While the evidence does not prove the SBN was meant to be a learning tool, its actions show how contemporary proxy warfare naturally creates a system that learns and adapts.

5. The Paradox: Cheap Experimentation Vs. Loss of Control

The exact traits that make this network cheap and agile also make it incredibly difficult for a sponsor to control.

A conventional militant organisation requires massive investments in training, leadership, weapons, and long-term maintenance. Losing trained personnel is a huge loss. A fragmented network like the SBN greatly reduces this risk. Because operatives are hired for isolated tasks, a single arrest does not jeopardize the whole system; the individual is simply replaced. With online recruitment, this creates a model of "cheap experimentation." The sponsor can test different tactics with lower risk.[12]

Even though a network becomes more disposable, the sponsor loses the ability to manage individual actors. Traditional proxies rely on clear chains of command and identifiable leadership, making them easier to monitor. Loosely connected digital recruits often have mixed motivations, lower competence, and no understanding of the broader objective. This creates severe operational risks: security becomes weak, information leaks easily, and operatives act unpredictably. A sponsor cannot simply maximize flexibility; they must constantly balance deniability, adaptability, and operational control.[13]

6. From Terrorist Networks to an Adaptive Proxy Ecosystem

Traditional terrorist groups are easy to understand because they have a clear hierarchy, fixed members, and obvious leaders. A modern proxy network doesn't rely on one single, permanent group, it mixes and matches different people for different jobs. The SBN combines handlers in Pakistan, local street gangs, and random internet recruits. This allows a sponsor to draw on different skills as needed.[14]

This network becomes "adaptive" because it changes whenever it faces pressure and can easily swap out compromised people, change tasks, or switch communication channels based on what is happening on the ground.[17]

Counterterrorism forces now have to target the underlying system; the digital tools and connections that allow remote hiring, funding, and quick rebuilding to happen. This network model isn't perfect, being decentralized means bad coordination, unreliable recruits, and a massive loss of control for the sponsor. This doesn't mean traditional terrorist groups are gone, it just adds a highly flexible model where jobs can be passed around and replaced across a massive web of people.[15]

7. The Road Ahead

If the SBN model keeps evolving, future proxy warfare will become increasingly decentralized, task-based, and quick to rebuild.[16] Based on its structure, we can predict three possible future paths**.**

Most likely, organizations will keep using cheap online hiring for quick attacks instead of building big terror groups. It does not matter if this specific network (the SBN) falls apart, what matters is that the method works. Things to watch out for include continuous online recruitment, a steady supply of new hires, and new networks copying this exact style.[17]

The next situation that is moderately likely to happen is that these loose networks keep messing up due to bad recruits or leaked info, and the sponsor might step in to fix them. They would introduce tighter security and stricter control. This would create a hybrid threat: a network that stays flexible but acts with the discipline of a traditional military proxy, but this is hard to do because professional training costs time and money; the very things this cheap model tries to avoid.[21]

Finally, if this online setup gets advanced enough, the sponsor could turn it into an all-in-one weapon for spying and sabotage, not just terrorism. This is unlikely because running a multipurpose network requires massive effort.

However, if it happens, the impact would be devastating: shutting down one cell would not stop the rest of their operations.[18]

These three paths can happen at the same time. The model will persist, while parts of it might diversify. The future of proxy warfare will depend less on the survival of any single group, and more on a sponsor's ability to constantly churn out new ones.

8. What this means for India’s National Security

- **Shift to Ecosystem-Centric Counterterrorism:** We cannot defeat these new networks by just arresting a single leader or busting a single cell. While India's current security strategies, like the Multi-Agency Centre (MAC) and the 2026 PRAHAAR strategy, already track online radicalisation and illegal weapons, counterterrorism forces must target the underlying engine: the online hiring platforms and the underworld logistics that allow these groups to constantly rebuild themselves.[19]

- **Disrupt the feedback loop:** If proxies are using our security reactions to study our defences, our counter-actions accidentally turn into their intelligence report. This doesn't mean we stop making arrests. The new goal is to stop the sponsor from figuring out why they got caught. We must connect the dots across different cases early to spot recurring digital footprints, just like the National Investigation Agency (NIA) did in January 2026 when they used social media trails to identify and disrupt online radicalisation modules.[20]

- **Strengthen coordination across agencies:** Terrorism, organized crime, and digital recruitment are the same hybrid threat. A shady internet message looks like a cyber issue, and a money transfer looks like a financial fraud case. They are all connected. While the PRAHAAR framework already calls for teamwork, agencies need to strengthen information-sharing across these areas.[21]

- **Build resilience against regeneration:** Even if we completely wipe out the SBN, a different handler can copy their idea tomorrow. True success means breaking the environment that allows these networks to respawn. Indian counterterrorism must shift from dismantling organizations to disrupting ecosystems.

Conclusion

This article indicated that the Shahzad Bhatti Network serves as a prime example for how proxy warfare is changing. Pre-existing criminal networks are blended with online recruitment to hire people for isolated tasks. Every single operation forces a response from the target state, which can be analysed. We have no definitive evidence that the SBN was intentionally built to be a learning laboratory, but its real-world execution shows how this feedback loop can emerge through repeated operations.

The bigger takeaway is that future threats will rely on flexible networks that can rapidly recruit new operatives, execute one-off tasks, learn from their mistakes, and regenerate the moment they are disrupted. The challenge for India is stopping these low-level operations from turning into a training school that exposes the country’s security blind spots.

The defining question is no longer whether a proxy can be defeated on the ground, but whether we can stop the adversary from learning how to defeat the target more effectively next time.

References:

[1] Stephen Watts et al., *Proxy Warfare in Strategic Competition: State Motivations and Future Trends* (Santa Monica, CA: RAND Corporation, 2023), 1–2.

[2] Watts et al., *Proxy Warfare in Strategic Competition*, 1–2.

[3] Watts et al., *Proxy Warfare in Strategic Competition*, 4–5.

[4] Alok Singh, “Beyond the Borders: The Pakistani Gangster Using Social Media to Build a ‘Shadow

Army’ of 300 Within India,” *The Indian Express*, May 11, 2026; Ministry of Home Affairs, Government of India, “Modi Government Destroyed the ISI-Backed Terror Group Shahzad Bhatti Network… by Arresting More Than 200 Operatives,” Press Information Bureau, August 17, 2026.

[5] Alexandra Stark, “Complicating the Proxy War Model,” in *Forum: Conflict Delegation in Civil Wars*, *International Studies Review* 23, no. 4 (2021): 2060.

[6] Candace Rondeaux and David Sterman, “Twenty-First-Century Proxy Warfare,” in *Understanding the New Proxy Wars: Battlegrounds and Strategies Reshaping the Greater Middle East*, ed. Peter Bergen, Candace Rondeaux, Daniel Rothenberg, and David Sterman (New York: Oxford University Press, 2022), 25–28.

[7] Singh, “Beyond the Borders.”

[8] Mohamed Thaver, “How Pakistan-Based Handlers Are Turning Vulnerable Indian Teens into Recruits,” *The Indian Express*, August 18, 2026.

[9] Singh, “Beyond the Borders”; Thaver, “How Pakistan-Based Handlers.” [10] Ministry of Home Affairs, “Modi Government Destroyed.” [11] Stark, “Complicating the Proxy War Model,” 2060–61.

[10] Alexandra Stark, “Complicating the Proxy War Model,” 2061–62.

[11] Alexandra Stark, “Complicating the Proxy War Model,” 2061.

[12] Watts et al., *Proxy Warfare in Strategic Competition*, 113–115; Thaver, “How Pakistan-Based Handlers.”

[13] Watts et al., *Proxy Warfare in Strategic Competition*, 113–115.

[14] Watts et al., *Proxy Warfare in Strategic Competition*, 113–115; Vijaita Singh and Devesh K. Pandey, “Gangster Shahzad Bhatti picked operatives through social media,” *The Hindu*, August 17, 2026. [17] Watts et al., *Proxy Warfare in Strategic Competition*, 113–114.

[15] Watts et al., *Proxy Warfare in Strategic Competition*, 113–115.; Stark, “Complicating the Proxy War Model,” 2061–62.

[16] Watts et al., *Proxy Warfare in Strategic Competition*, 114–115; Thaver, “How Pakistan-Based

Handlers.”

[17] Ministry of Home Affairs, “Modi Government Destroyed”; Thaver, “How Pakistan-Based Handlers.” [21] Watts et al., *Proxy Warfare in Strategic Competition*, 114–116.

[18] Singh, “Beyond the Borders.”

[19] Ministry of Home Affairs, Government of India, *National Counterterrorism Policy & Strategy*, February 23, 2026.

[20] National Investigation Agency, “NIA Charges 5 Accused in Gujarat AQIS Online Radicalisation Case,” January 17, 2026.

[21] Ministry of Home Affairs, *National Counterterrorism Policy & Strategy*.

The views expressed are those of the authors and do not represent the views of CNAWS.

?ImageSource: ChatGPT