DETAILED REPORTS

Recursive Proxies: The Hybrid Face of Terrorism in Jammu & Kashmir

Author: Mohit Vashisth • **Published:** October 25, 2025 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Pakistan's proxy-war architecture in Jammu and Kashmir is no longer confined to terrorist groups operating across physical terrain. It has evolved into a multilayered ecosystem in which Lashkar-e-Taiba and Jaish-e-Mohammed retain the kinetic capability, while digital fronts such as The Resistance Front, People's Anti-Fascist Front and Kashmir Tigers claim attacks, shape narratives and project cross-border terrorism as indigenous resistance. Reinforced by unofficial online mouthpieces, these "recursive proxies" create successive layers of deniability, blur attribution and transform information warfare into an integral component of Pakistan's terrorist strategy.

The landscape of terrorism in Jammu and Kashmir (J&K) has undergone a profound structural transformation in recent years. The nature of terrorism in Jammu and Kashmir (J&K) is no longer defined only by covert infiltration or cross-border sponsorship. The familiar proxy model where Pakistan directly supports terrorist outfits such as Lashkar-e-Taiba (LeT) or Jaish-e-Mohammed (JeM) has evolved into something far more complex and adaptive. Since 2019, Pakistan's asymmetric strategy has entered a new phase where violence and information warfare merge into one hybrid campaign. The traditional terrorist organizations continue to serve as the operational backbone of this effort. Yet, a new layer has emerged above them i.e., a set of entities that exist largely in the digital space, claim attacks conducted by the old

groups, and project those acts as part of an indigenous, political resistance.

The Resistance Front (TRF), People's Anti-Fascist Front (PAFF), and Kashmir Tigers (KT) illustrate this transformation. They represent what may be termed recursive proxies, a new phenomenon where existing proxies reproduce themselves through digitally enabled fronts that manage narratives, obscure attribution, and reinforce plausible deniability. A further adaptation has introduced another layer consisting of unofficial mouthpieces such as Jhelum Media House, Kashmir Fight, Kashmir Conflict, Kashmir Media Network, and Zuv Magazine. These handles serve as informal amplifiers for recursive proxies, occasionally claiming responsibility for incidents with high civilian casualties, after which TRF or PAFF publicly deny involvement. This additional layer increases confusion, diffuses accountability, and refines the art of denial in the information domain.

This evolution represents a strategic recalibration by Pakistan's deep state in response to international scrutiny, domestic pressures, and changing technologies of warfare. It blurs the lines between state sponsorship, terrorism, militancy, and local insurgency in a way that conventional counterterrorism frameworks struggle to comprehend.

The years following the abrogation of Article 370 and Pakistan's placement on the Financial Action Task Force (FATF) grey list forced Islamabad to rethink its method of conducting its long-standing proxy campaign. Open support to terrorist groups carried escalating diplomatic and economic costs. The response was a reconfiguration of its terrorist architecture into a dual system, where traditional terror outfits retained operational control while a new generation of digital fronts managed public communication and ideological framing.

Understanding the Hierarchy

1. ISI and Pakistani Army: The strategic sponsors directing funding, training, and operational oversight.
2. Core Kinetic Proxies: LeT and JeM: The operational arms that handle recruitment, logistics, planning, and attack execution. Their leadership and command structures remain intact.
3. Recursive Proxies: TRF, PAFF, KT: Narrative fronts that claim attacks, glorify terrorists, announce "martyrs," and disseminate propaganda. They were introduced post-2019 to build local legitimacy and construct a digital shield of deniability for Pakistan's core terror networks.
4. Unofficial Mouthpieces (e.g., Jhelum Media House, Kashmir Fight, Kashmir Conflict, Kashmir Media Network, Zuv Magazine): Social media outlets that amplify or sometimes claim responsibility for attacks, particularly those resulting in civilian casualties. Their later disavowal by the recursive proxies adds another layer of plausible deniability and confuses attribution.

The Post-2019 Shift: From Battlefields to Narratives

The years following the abrogation of Article 370 and Pakistan's grey-listing by the FATF represented a moment of reckoning for Islamabad's proxy strategy in J&K. Traditional terrorist groups such as LeT, JeM, and Hizbul Mujahideen had come under intense international scrutiny. Their financial channels were disrupted, their networks exposed, and their foreign hand was undeniable.

Faced with mounting pressure and the risk of formal blacklisting, Pakistan's Inter-Services Intelligence (ISI) adopted an adaptive strategy. Rather than dismantle the existing proxy infrastructure, it sought to repackage it. New terrorist "fronts" were floated to create distance between Pakistan and the attacks, while still retaining complete operational continuity through LeT and JeM.

The logic was straightforward:

- Operational continuity would remain with LeT and JeM, whose leadership and logistical networks were intact.
- Narrative control would shift to newly created entities like TRF, PAFF, KT, and others that appeared local, secular, and organic.
- International optics would shift from cross-border terrorism to “local resistance.”

This dual structure comprising of kinetic and digital actors gave birth to a recursive model of terrorism in Kashmir: a hybrid ecosystem where violence on the ground and propaganda in cyberspace reinforce each other in real time.

Defining and Establishing the Concept of Recursive Proxies

The term recursive proxy refers to a phenomenon in which an existing proxy organization, instead of conducting public operations under its own name, deploys or enables secondary fronts that assume responsibility for acts it continues to carry out. In mathematics and computer science, recursion denotes a process that refers back to itself. Borrowing that logic, the term *recursive proxy* captures how terrorist organizations reproduce their presence within new digital identities that refer indirectly back to the original network.

A recursive proxy is therefore *a representational extension of a core terrorist organization, functioning as a narrative and informational façade that claims operational acts executed by the parent entity, thereby multiplying layers of deniability and legitimacy.*

This definition rests on four principles.

1. **Origin within an existing proxy structure:** Recursive proxies do not emerge independently. They originate within an already established proxy network. In J&K, TRF, PAFF, and KT emerged from within LeT and JeM ecosystems under the strategic direction of the ISI.
2. **Division of labor between kinetic and narrative domains:** Operational violence remains the responsibility of the parent organization. The recursive proxy functions in the information domain, claiming attacks, managing propaganda, and cultivating ideological appeal.
3. **Recursive reproduction of identity:** Each layer reproduces the objectives and narratives of the previous one but under new names and idioms. This recursion allows the same network to appear as multiple distinct entities, creating analytical confusion for law enforcement and observers.
4. **Function of deniability and legitimacy:** By interposing digital intermediaries, Pakistan achieves what can be called *plausible deniability 2.0*. The recursive proxy allows the sponsor and the core organizations to appear detached from specific incidents, while simultaneously projecting the violence as an indigenous political movement.

The term recursive proxies therefore defines a new class of actors in proxy warfare, extending the traditional dyadic sponsor-proxy relationship into a multilayered system that integrates information operations. Classical proxies acted as physical surrogates for their sponsors. Recursive proxies and their mouthpieces act as informational surrogates, transforming proxy warfare into a hybrid construct where controlling the narrative becomes as decisive as controlling terrain.

This conceptualization extends traditional literature on proxy warfare, which has generally assumed a linear structure between the sponsor and the surrogate. Most classic studies of proxy war, from Andrew Mumford’s *Proxy Warfare and the Future of Conflict* (2013) to Eli Berman and David Lake’s work on delegation and control, describe the sponsor-proxy relationship as dyadic. In contrast, recursive proxies introduce triadic and multilayered relationships, adding an

information domain intermediary that manages legitimacy and deniability simultaneously.

The term also aligns with theories of hybrid warfare, where non-linear combinations of military, informational, and political means are used to achieve strategic goals below the threshold of open war. Recursive proxies embody this hybridity at the micro-level of terrorist communication, fusing terror and narrative into a single recursive feedback system.

By establishing this term, the intent is not merely to name a new group of actors but to define a structural feature of twenty-first-century proxy conflict. Just as scholars once distinguished between “state-sponsored” and “state-enabled” terrorism, the notion of recursive proxies identifies the emergence of *state-enabled digital surrogates* that sustain older terrorist networks under contemporary constraints.

Defining the Additional Mouthpiece Layer

Unofficial mouthpieces are social-media handles and channels that disseminate, and sometimes originate, provocative claims and content. They are often less formal, more volatile, and more willing to embrace graphic or sensational claims than the recursive proxies whose messaging they amplify.

The addition of this fourth tier changes the dynamics of recursion. The parent organization persists as the kinetic core, the recursive proxy functions as the official narrative claimant, and unofficial mouthpieces act as a third-order diffusion mechanism. The mouthpieces sometimes step beyond the scripts preferred by the sponsor and claim responsibility for incidents that involve large numbers of civilian casualties. Their provocative claims generate international attention and condemnation. At that point the recursive proxies issue denials or distance statements, claiming no involvement. This sequence produces a layered confusion: an initial claim from an unofficial source, subsequent denial by the recursive front, and an enduring ambivalence in the public record that weakens attribution and complicates accountability.

Theoretical Foundations

The recursive proxy phenomenon can be situated within five interlinked theoretical frameworks that together explain its logic of emergence and persistence.

Principal–Agent Theory:

As Kathleen Eisenhardt noted, “one party (the principal) delegates work to another (the agent)” (Eisenhardt, 1989). The ISI and the Pakistani Army act as principals delegating violent operations to LeT and JeM. Under pressure, these agents further delegate the representational function to digital fronts, creating an additional tier of agency. Each new layer increases information asymmetry, allowing the sponsor to distance itself from observable responsibility while retaining control over outcomes. The recursive proxy is therefore a by-product of multilayered delegation designed to diffuse accountability across domains.

Network Theory and Structural Holes:

Ronald S. Burt’s network theory is instructive here. He observed that “the basic element is the structural hole: a gap between two individuals with complementary resources or information” (Burt, 1992). Recursive proxies act as bridges across these structural holes, connecting the terrorist ecosystem with different audiences i.e., local populations, international observers, and online sympathizers while concealing the true operational nodes. In doing so, they broker meaning and control flows of information between otherwise disconnected communities. Their apparent independence hides the relational overlap with core organizations, giving Pakistan an additional layer of informational insulation.

Information Warfare and Signalling:

The behaviour of recursive proxies can also be understood through signalling theory and the literature on information warfare. John Arquilla and David Ronfeldt described modern networked conflict as one in which “the antagonists are organized more as sprawling ‘leaderless’ networks than as tight-knit hierarchies” (Arquilla & Ronfeldt, 1996). TRF, PAFF, and KT function precisely in this manner: decentralized, agile, and capable of controlling the first narrative after every violent incident. When a terrorist attack occurs, these digital fronts release statements or visuals within hours, shaping perception before any verification can take place. This rapid signalling reframes cross-border terrorism as an indigenous resistance struggle, exploiting what Michael Spence’s signalling theory would describe as the asymmetry of information between sender and receiver.

Organizational Ecology and Diffusion:

From the standpoint of organizational ecology, groups adapt when environmental conditions threaten their survival. Michael T. Hannan and John Freeman’s population ecology of organizations explains that environmental constraints select for new organizational forms. Everett M. Rogers’ work on diffusion complements this by noting that “diffusion of innovations is a social process” (Rogers, 1962). When LeT and JeM came under global pressure, the digital fronts emerged as new organizational forms occupying an unregulated niche. Their appearance diffused rapidly across terrorist communication networks because the template worked: new names, secular narratives, and plausible deniability allowed continued operations with reduced external risk.

Complex Adaptive Systems:

John Holland described complex adaptive systems as “systems composed of interacting agents described in terms of rules” (Holland, 1992). The proxy network in J&K fits this model: multiple interacting agents (sponsor, proxies, recursive fronts, and audiences) whose local interactions produce resilience and adaptation. Recursive proxies emerge as the system’s self-organizing mechanism to preserve continuity under stress. Each time India or the international community targets one component, the system reorganizes through digital mutation rather than collapse. Recursive proxies are the system’s adaptive response to environmental stress, ensuring continuity through diversity and self-replication.

Why the Recursive Proxy Model Emerged in J&k

The rise of recursive proxies in J&K can be explained by three interlinked strategic imperatives driving Pakistan’s recalibration.

1. **Plausible Deniability 2.0:** In the post-9/11 era, global counterterrorism mechanisms made overt sponsorship of terrorist groups politically untenable. FATF scrutiny further constrained Pakistan’s ability to support proscribed organizations directly. Recursive proxies act as an additional buffer, providing Pakistan with “plausible deniability 2.0.” When a new front like TRF or PAFF claims responsibility, Islamabad can distance itself by arguing that these groups have no formal connection to banned entities.
2. **Narrative Diversification and Digital Rebranding:** By adopting names and symbols that resonate with local or secular sentiments, recursive proxies attempt to rewrite the story of terrorism in J&K. The very term “resistance” evokes political struggle rather than terrorism or cross-border jihad. This semantic shift aims to repackage terrorism as activism, appealing to younger demographics radicalized through online spaces rather than traditional religious networks.

3. **Organizational Resilience and Network Continuity:** Recursive proxies act as insurance mechanisms for terrorist ecosystems. When a parent proxy's leadership is neutralized or its assets are frozen, these newer fronts preserve institutional memory, recruitment pipelines, and ideological coherence. They ensure continuity of operations even under sustained counterterrorism pressure.
4. **Information Dominance:** Recursive proxies became tools for narrative synchronization. As kinetic attacks were conducted by LeT and JeM cells, TRF or PAFF would swiftly claim responsibility online, issue martyrdom statements, shape social media discourse and projecting control over the battlespace of information.

How the Recursive Model Functions

LeT and JeM continue to conduct kinetic operations: recruitment, training, funding, and attacks. Once an operation is executed, TRF, PAFF, or KT immediately claim responsibility, publish imagery, and manage online discourse. These fronts glorify their "fallen fighters," release slick videos, and frame the violence as political resistance. The shift is not only in message but in method: official LeT and JeM media outlets have gone silent, replaced by agile digital surrogates that speak the same language through modern, secular vocabulary.

This separation of operational execution from narrative ownership is the defining attribute of recursive proxy warfare. The act and the claim now exist in different domains, one physical and one informational, but serve the same strategic purpose. It represents a sophisticated evolution of Pakistan's information operations in Kashmir.

They obscure the real source of attacks. By attributing incidents to TRF or PAFF, LeT and JeM maintain operational secrecy and political deniability. They shape online discourse by releasing attack videos, martyrdom posters, and fabricated "communiqués" on social media that are often designed to evoke local grievances and global solidarity. They magnify fear and confusion through disinformation by spreading fake reports, distorted casualty figures, or exaggerated claims to dominate the narrative space post-attack. They create recursive feedback loops (terrorist operations feed propaganda, propaganda fuels recruitment, and recruitment sustains operations) thus making the network self-reinforcing across both domains.

How the Mouthpieces Work with Recursive Proxies

Operationally, the system produces a repeating sequence after a violent event. An attack occurs. Evidence in the field shows operational signatures consistent with LeT or JeM activity. Within a short window, often hours, an unofficial mouthpiece posts initial claims, graphic footage, or raw assertions that frame the incident in the most provocative terms. These posts are designed to maximize shock value and to place the issue on the international and social-media agenda. If the claimed incident includes significant civilian casualties or creates a level of political blowback that would be damaging to the larger strategy, recursive proxies will either refrain from claiming the attack or will later publish statements denying involvement. This staged sequence performs three functions. It tests whether a sensational claim will stick in public discourse. It gauges international response. And it affords a subsequent opportunity for controlled disavowal when necessary. The deliberate ambiguity sows doubt in attribution and increases the cost of international retaliation or diplomatic measures that require clear evidence of state-sponsored aggression.

They have occasionally claimed responsibility for incidents that produced civilian casualties, after which TRF and PAFF issued denials or clarified they had no role. That pattern illustrates how the system uses an additional layer of separation not only to obscure links but to modulate the narrative after testing audience responses. The mouthpieces are intentionally more expendable and less traceable to formal organizational media wings, which further complicates

efforts to trace content provenance and responsibility.

Implications

The battleground in J&K now extends beyond terrain and tunnels into data and discourse. Control over perception (who claims an attack, how it's framed, and how quickly narratives spread) has become as critical as the act of violence itself.

The emergence of recursive proxies changes how terrorism must be analyzed and countered. Attribution becomes multidimensional, requiring investigators to connect digital claims with physical acts. India's proscription model targets organizations by name. Recursive fronts exploit this by rebranding faster than legal instruments can adapt. A name-based approach to terrorism designations is inadequate for a recursive system that reproduces itself under new labels. Legal frameworks that proscribe organizations by name must evolve toward function-based designations encompassing narrative arms and successor entities. Counterterrorism policy must recognize that neutralizing physical networks without addressing their digital mirrors achieves only partial success. Any entity functioning as a successor, affiliate, or propaganda arm of a designated group must automatically fall under the same legal sanctions.

For India's intelligence community, this means integrating OSINT and SOCMINT more systematically. These fronts saturate digital ecosystems with propaganda, memes, and fake communiqués. The flood of content challenges open-source intelligence (OSINT) analysts, who must distinguish authentic material from deliberate deception. Mapping relational overlaps in digital content, language patterns, and dissemination networks can reveal the underlying recursion linking these fronts to their parent organizations. Publicly exposing these links also serves a strategic communication function, stripping away the mask of local legitimacy that Pakistan seeks to construct.

For scholars, the recursive proxy phenomenon offers a new analytical lens for hybrid warfare and information operations. It suggests that the future of terrorism studies must integrate insights from network science, information theory, and complex systems. The recursive model is not unique to J&K; similar patterns can emerge wherever terrorist ecosystems face external constraints but retain communication access to global audiences. The mouthpiece phenomenon suggests several testable propositions. The frequency of mouthpiece claims should increase after spikes in international scrutiny of a sponsor or its proxies. The lag between a mouthpiece claim and a recursive-proxy denial should correlate with the intensity of international backlash. Content analysis will reveal stylistic and production markers that tie mouthpiece outputs to the infrastructure or personnel networks of recursive proxies and their operational cores. These are empirical hypotheses that can be evaluated using carefully collected OSINT, metadata analysis, and where possible, human-source corroboration.

Conclusion

The concept of recursive proxies provides a new lens to understand how Pakistan has adapted its long-standing proxy warfare in J&K to the realities of global scrutiny and digital media. It identifies a structural innovation in the architecture of terrorism, one that replaces overt organizational branding with fluid, self-replicating digital fronts. In this hybrid environment, the boundary between the gun and the keyboard has dissolved.

By defining and theorizing recursive proxies, this article establishes a foundational framework for future study of hybrid terrorist networks. Recognizing these entities for what they are is essential for designing both analytical tools and policy responses.

Pakistan has created an ecosystem of plausible deniability that thrives in the age of instant information. Recognizing these fronts as recursive proxies provides conceptual clarity and strategic direction. Countering them will require India to

extend its fight from the battlefield to the information sphere, combining kinetic precision with narrative control. The war in Kashmir is now fought as much in the mind as on the map, and victory will depend on who shapes the story first.

References:

Arquilla, John, and David Ronfeldt. *The Advent of "Netwar."* RAND Corporation, 1996.

Berman, Eli, and David A. Lake. *Proxy Wars: Suppressing Violence Through Local Agents.* Cornell University Press, 2019.

Burt, Ronald S. *Structural Holes: The Social Structure of Competition.* Harvard University Press, 1992.

Eisenhardt, Kathleen M. "Agency Theory: An Assessment and Review." *Academy of Management Review* 14, no. 1 (1989): 57–74.

Hannan, Michael T., and John Freeman. "The Population Ecology of Organizations." *American Journal of Sociology* 82, no. 5 (1977): 929–964.

Holland, John H. "Complex Adaptive Systems." *Daedalus* 121, no. 1 (1992): 17–30.

Mumford, Andrew. *Proxy Warfare and the Future of Conflict.* Polity Press, 2013.

Rogers, Everett M. *Diffusion of Innovations.* Free Press, 1962.

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