Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 3, 2026

HYBRID WARFARE IN BALOCHISTAN: MULTI-DOMAIN STRATEGIC COMPETITION, NATIONAL SECURITY CHALLENGES, AND POLICY OPTIONS FOR PAKISTAN

Sher Dil Khan[*1], **Prof. Dr. Robina Yasmin**[2]

[*1]*PhD Scholar, Department of Pakistan Studies, The Islamia University of Bahawalpur, Bahawalpur*
[2]*Chairperson, Department of Pakistan Studies, The Islamia University of Bahawalpur, Bahawalpur*

[*1]sherdil114@yahoo.com

DOI: http://doi.org/10.5281/zenodo.23834963

Keywords
Hybrid Warfare; Balochistan; National Security; Resilience; CPEC; Securitization

Article History
Received: 20 January 2026
Accepted: 19 February 2026
Published: 05 March 2026

Copyright @Author
Corresponding Author: *
Sher Dil Khan

Abstract

Balochistan's strategic location, resource base and position within the China–Pakistan Economic Corridor (CPEC) make its persistent insecurity consequential for Pakistan's national security. Yet insurgency, political grievances, economic disruption and digital influence are often analysed separately, obscuring interactions without proving that all originate in a single coordinated campaign. Using qualitative documentary analysis for 2001–2026, this article examines how domestic vulnerabilities and cross-border pressures can combine across military, political, informational, economic, cyber, diplomatic and societal domains. Theory of 'hybrid warfare' offers the main analytical frame, and theory of 'securitization' explains rival threat representations and the resilience literature the policy response. Official Pakistani policy documents, census and human-development evidence, institutional project records and security reporting are assessed against a cautious attribution standard. The analysis identifies a set of pathways that explain how the effects of violence and geopolitical competition become manifested in the form of political legitimacy, unequal access to services, protection of critical infrastructure, and credible communication. It proposes an integrated, civilian-accountable resilience framework linking intelligence coordination, constitutional participation, equitable development, digital preparedness and regional diplomacy. The study adds an explicitly conditional model of multi-domain security that does not presume that simultaneous threats are part of an orchestrated hybrid campaign.

Introduction

Balochistan connects Pakistan's western land frontier, Arabian Sea coastline and potential trade routes towards Afghanistan, Iran and Central Asia. Its ports, mineral resources and transport corridors intersect domestic development priorities with external economic and strategic interests. The China-Pakistan Economic Corridor Secretariat lists the port and free zone of Gwadar, the vocational institute, the hospital, the desalination projects, and the Eastbay Expressway as some of the available projects, which demonstrates the wide range of development-security linkages but does not mean that each project has yielded expected results (China-Pakistan Economic Corridor Secretariat, n.d.). As Pakistan's largest province by area, Balochistan also poses distinctive administrative challenges arising from dispersed settlements, long distances and unequal service access (Pakistan Bureau of Statistics, 2025).

It is not an external conspiracy, nor is it as simple as lack of domestic resources, that is the

security problem. Militancy and attacks on infrastructure create direct costs, but political exclusion, inadequate services and contested distribution of development benefits can shape popular responses. Equally, transboundary movements, regional rivalries and digital networks create opportunities for violence and influence that exceed provincial boundaries. The government's National Security Policy (2022-2026) raises economic security alongside citizens' welfare to a broader security policy. According to this citizens' welfare becomes a policy lever to consider these relationships (NSD, 2022). This article enquires about the security environment of Balochistan from 2001 to 2026 and how vulnerabilities converge and interact with pressures along seven dimensions, and then asks what types of institutional responses might diminish the pressure from vulnerabilities. Its contribution is analytical discipline: the presence of terrorism, a contested narrative and economic difficulties at the same time does not itself prove strategic coordination among actors. Hybrid warfare is not a term that is used as an exhaustive description of unrest; it is offered as a possible interpretation. The discussion remains focused on Balochistan, bringing in Pakistan-wide or regional evidence only where it illuminates provincial conditions.

Literature Review and Theoretical Framework

Hoffman (2007) defined the concept of hybrid conflict as the mixing of conventional capabilities, irregular tactics, and terrorism and criminality in the same battlespace. Subsequent institutional understandings emphasize overt and covert instruments beyond armed force. NATO (2026) characterizes hybrid threats as combinations of military and non-military means, including disinformation, cyberattacks and economic pressure. The emphasis is different in these definitions: while Hoffman is developing a mode of conflict, policy use in the present tends to produce a more expansive definition of the set of tools for hostile influence. Using them interchangeably risks classifying routine diplomacy, political dissent or structural poverty as hostile warfare.

The emphasis is different in these definitions: while Hoffman is developing a mode of conflict, policy use in the present tends to produce a more expansive definition of the set of tools for hostile influence. This distinction matters particularly when considering allegations of foreign sponsorship, cyber disruption and information manipulation. Opposition to a development project does not constitute disinformation and it is an accepted principle that peaceful political protest is an acceptable method of campaigning but it does not represent coercive violence. Securitization theory is about a different query: how political actors make issues appear as an emergency threat that requires exceptional reactions. Buzan et al. (1998) explain securitization through threat claims, audience acceptance and extraordinary measures. Applied to Balochistan, this lens draws attention to the consequences of representing development disputes, migration, infrastructure protection or protests primarily as security emergencies. Such framing may mobilize resources but can also narrow political engagement. Securitization is therefore a complement to, not evidence for, hybrid-warfare claims.

Instead of focusing on a single measure of success, the number of attacks averted, resilience assesses an institution's or community's capacity to predict disruption, provide critical services, adjust and rebuild trust. Pakistan's National Cyber Security Policy 2021 calls for institutional coordination, incident response and sectoral security arrangements, furnishing a concrete illustration of systemic preparedness (Ministry of Information Technology and Telecommunication, 2021). A resilience perspective further requires transparent governance, lawful enforcement and local participation, because technical protection without public legitimacy offers limited durability.

The integrated conceptual sequence is thus: structural vulnerability creates exposure; identified actors may exploit exposure through mutually reinforcing instruments; interactions alter security, governance and economic outcomes; and institutional resilience moderates those impacts. This sequence allows alternative explanations. An infrastructure attack may be an insurgent attack without any

cyber coordination; a misleading online story may be local not overseas; an infrastructure project may create social contention, even if there is no hostile actor. The framework is falsifiable and does not claim correlation as attribution by breaking down cause, action and effect.

Research Methodology and Limitations

The article uses qualitative, document-based thematic analysis, organized chronologically and by security domain. The period begins in 2001 because the Afghanistan war and subsequent counterterrorism environment affected Pakistan's western borderlands; it ends in 2026, the study's documentary cutoff. Primary institutional documents include the National Security Policy, National Cyber Security Policy, the China–Pakistan Economic Corridor Secretariat's official project inventory and the 2023 population census provincial report. The published indicator analysis provided by UNDP's National Human Development Report and the structured accounts of militant violence provided by Pak Institute for Peace Studies (PIPS) report are provided by the Pak Institute for Peace Studies (PIPS) report (China–Pakistan Economic Corridor Secretariat, n.d., 2021; NSD, 2022; PBS, 2025; PIPS, 2026; United Nations Development Programme, 2024). Sources were assessed by proximity to the event, the institution's competence to report it and the distinction between observed incidents and interpretive claims. Administration policy is the official evidence of government commitment, not proof of policy execution. Incident reports are evidence of violence that has occurred and cannot prove sponsorship or coordination of violence perpetrators independently. Thematic categories were military, political, informational, economic, cyber, diplomatic and societal; the cross-domain synthesis identifies mechanisms rather than duplicating seven inventories of consequences.

The limitations are significant. This is neither fieldwork nor an interview-based account, and it does not access classified intelligence, digital-forensic attribution or district-level causal data for the full 25-year period. The seven-domain scheme is an analytical choice, not a claim that every domain was equally affected. Findings do not provide estimates of the percentage of insecurity caused by hybrid operations, but rather plausible explanations and policy priorities. The evidence of a foreign manipulation should be investigated on the basis of independently examinable evidence, not by strategic rivalry alone.

Evolution of Baluchistan's Security Environment, 2001–2026

The first phase was in general (2001-2008) which saw the impact of the conflict in Afghanistan, along with the resurgence of Baloch insurgency in the mid-2000s. Border mobility, armed militancy and local disputes occurred alongside demands concerning political representation and resource distribution. The conflict was not a new phenomenon created by the global counterterrorism campaign; historical grievances predated it. The analytic significance of 2001 is that international counterterrorism practices and changing regional networks added pressures to an existing provincial political crisis. Such disadvantaged instances are a part of the matter and that is without a doubt essential for a reputable historical past.

During 2009–2015, internal insecurity acquired additional sectarian, militant and infrastructure-related dimensions. Armed groups had many aims and cannot be shown to be acting in concert. The announcement and early implementation of CPEC also elevated the security importance of routes, potential industrial activity and coastal development. Accordingly, government attention increasingly encompassed project protection and coordination between civilian and security institutions. Yet protective deployment could not by itself resolve disputes over provincial authority, access to employment or allocation of economic benefits.

The 2016–2020 period saw the continuing strategic prominence of CPEC and Gwadar. Official planning related to port infrastructure, connectivity and municipal services made development a central political and security issue (China–Pakistan Economic Corridor Secretariat, n.d.). Threats to economic assets could impose costs beyond immediate damage

by raising insurance, operational and investor concerns. But it is highly not possible that disruption of investment will automatically be handed over to a foreign hybrid campaign. Administrative capacity, commercial feasibility, implementation delays and local consent may also influence outcomes. Given these points, a good assessment of security and development should necessarily give due consideration to distinguishing between intentional sabotage and key institutional or market barriers. Public records show that there has continued to be violence in Pakistan in these five years (2021-26) and there has been growing anxiety about potential digital weaknesses. PIPS (2026) document a marked nationwide increase in terrorist attacks in 2025, with implications for provincial security preparedness. That evidence establishes an escalating national terrorism environment but does not in itself demonstrate that physical attacks in Balochistan were synchronized with cyberattacks or overseas information operations. Similarly, Pakistan's 2021 cyber policy does not actually state whether Pakistan's domestic incidents were hybrid or not, but it states that there are systemic ICT risks within the borders of Pakistan (MoITT, 2021). The defensible conclusion is that Balochistan faces overlapping armed, governance, economic and information-related exposures, whose degree of coordination must be assessed case by case.

Across these phases, continuity is as important as change. Longstanding questions of political inclusion, resource rights and service delivery persist while the strategic significance of the coast, border and digital communications has grown. A simple linear story of 'traditional insurgency becoming hybrid war' overstates what public evidence can prove. It is easier to state it is now a more interdependent and critical conflict space where certain events have consequences apart from the immediate site of the conflict.

The Interaction of Seven Security Domains

Military and Internal Security Domain

Militant attacks against civilians, law-enforcement personnel, transport systems and development assets impose human and operational costs. Networked actors can exploit geographical distance, fragmented jurisdiction and weak information sharing. The military sphere can have disproportionate impacts when attacks disrupt commercial trafficking, or when communities and institutions become insecure. Yet counterinsurgency, counterterrorism and ordinary criminal enforcement require different legal standards and intelligence assessments. Cooperation among police, civilian administration, border agencies and military institutions can improve response, provided mandates and oversight remain clear. Protection of civilians and credible investigations are at the heart of sustainable security, not an extra humanitarian component.

Political Legitimacy and Governance

Political vulnerability does not just mean having elected representatives in place – it is about how responsive and fair institutions are towards them. Where decisions about land, resources, public spending or development are viewed as distant or opaque, contentious events can deepen distrust. Political solutions are required to take care of the grievances, whether or not they're exploited or no. Federal–provincial relations, accountable policing, local government authority and effective complaints procedures therefore shape security outcomes. In general, securitization theory suggests that every political discord can be read as a threat, which can increase alienation and diminish the state's ability to get reliable information from the community (Buzan et al., 1998).

Information and Narrative Competition

Information operations can broaden the consequences of a violent episode by spreading false claims, manipulative imagery or misleading accounts of responsibility. Networked platforms speed up distribution and corrects are tricky to implement after a loss of trust has occurred. NATO identifies coordinated harmful manipulation from a range of contentious information in its 2024 information-threat framework. For Balochistan, this distinction is vital: critical reporting, legitimate protest and calls for accountability are not automatically hostile narratives. Effective communication, backed up by definite

incident updates, clear correction of errors, a responsible approach to the local media and a proven responsibility for responsive governance, is the hallmark of good communication. Repealing or blocking investigations can backfire and may give rise to greater rumors, and decrease the credibility of the institutions.

Economic and Infrastructure Security

Gwadar, road links, electricity facilities, logistics systems and mineral extraction create opportunities but concentrate risk. The portfolio of the Secretariat of the China–Pakistan Economic Corridor includes the works of physical infrastructure as well as social facilities comprising healthcare, training and water-related projects, which will clearly demonstrate the success of the corridor beyond mere port and transport throughput. A security incident can halt construction, damage equipment or deter investment; a failure to distribute benefits fairly can also generate resentment independently of violence. Hence asset protection and social accountability are mutually reinforcing. Transparent contracts, local recruitment practices, environmental safeguards, compensation mechanisms and credible impact evaluations should accompany conventional physical security.

Cybersecurity and Digital Dependence

The expansion of connected government services, communications and infrastructure adds exposure to ransomware, intrusion, data theft and service interruption. Analytically, cyber-enabled propaganda is a propaganda manipulation of perception while an intrusion into operational technology is a compromise of systems. Pakistan's National Cyber Security Policy identifies national coordination, critical information infrastructure, sectoral response arrangements and technical workforce development as priorities (MoITT, 2021). In Balochistan the immediate priority is to determine which assets are genuinely critical and to test continuity arrangements. Until there are credible forensic evidence that supports the claim of General Cyber vulnerability, it cannot be written as proof of cyber campaign against Gwadar.

Diplomatic and Cross-Border Setting

Balochistan's adjacency to Afghanistan and Iran places local security within wider border governance, migration, trade and diplomatic negotiations. Administrative boundaries can be crossed by transnational smuggling or militant movement, and bilateral relations can be difficult, making evidence sharing challenging. Regional states might be competing for a strategic purpose without so many of such events turning into proxy warfare. Diplomatic efforts focus, therefore, on mechanisms whose results can be verified: border liaison mechanisms, legal mechanisms for exchanging information, trade facilitation mechanisms, and channels for addressing allegations between the two nations. It is not enough to attribute this sponsorship to another state, it involves a stronger evidentiary point than just a geopolitical interest in the western region of Pakistan.

Societal Cohesion and Human Security

Education, health, drinking water, employment and political voice are protective capacities that influence whether shocks develop into prolonged instability. Balochistan's human development index is 0.444 (UNDP, 2024) and there is significant variation between different districts; these are based on previous household survey data and cannot be misinterpreted as an assessment of conditions in 2026. Low development is not proof that a person will join militancy, but the persistence of service deficits can make security policies appear disconnected from everyday concerns. Young people, women, rural residents and fishing communities have differing experiences that provincial averages conceal. Social resilience requires locally responsive education, employment, healthcare and avenues for lawful participation.

These domains are connected via mechanisms, not a central command. An attack may disrupt transport, harm livelihoods and produce competing narratives; governance failures may amplify the reputational impact of that attack; a dependable response may contain those effects. But if you see something happen once and see criticism of the action somewhere else on the Internet, that doesn't necessarily mean that it is connected. The multi-domain approach comes

in very handy when it identifies both legitimate connections and limitations in attribution.

Drivers and Strategic Consequences

Internal drivers include administrative reach, unequal development, grievances concerning representation, weak access to justice and perceived inequity in the distribution of economic opportunities. Evidence from the National census shows the need for planning that is specific to each district and not to be assumed that a provincial intervention will be appropriate for every district (PBS, 2025). UNDP's disaggregated findings similarly show why Quetta, Gwadar and more remote districts cannot be treated as economically interchangeable (UNDP, 2024). These variables may make particular communities more exposed to political distrust and recruitment pressures, but causal pathways depend on local organizations, interpersonal networks and specific events.

External drivers include changes in Afghanistan, cross-border organized crime, regional strategic competition and technology-enabled communication. Different actors may independently benefit from a weakened security environment; common benefit is not conclusive evidence of coordination. Clearly separating enabling conditions from proven sponsorship helps avoid analysis biases due to confirmation and enhances policy targeting. Financial investigation and policing are required for criminal trafficking; prevention and prosecution are required for ideological militancy; and push-back depends on the use of diplomatic instruments when it comes to external pressure. Even if the consequences of two problems are the same, the evidentiary and operational requirements are different for each problem.

National-security implications extend beyond battlefield loss. Repeated attacks can burden public finances and security institutions, create uncertainty for investors and impair connectivity. Those governance mechanisms which exclude communities can undermine trust and inadequate protection of critical assets can derail nationally important development. Fragmented responses also impose coordination costs: police may focus on criminal accountability, project agencies on delivery deadlines, cyber authorities on networks and diplomats on border relations. National resilience is the ability to link these requirements and maintain each responsibility. The NSD's framework for economic and human security offers a basis for that broader approach, although documented policy aspiration cannot be equated with successful execution (NSD, 2022).

The CPEC relationship deserves particular caution. Infrastructure can support livelihoods, logistics and regional commerce; exposure of key assets also creates targets for violent disruption. Both arguments fail to show that local opposition to a project is manipulated from outside. A credible assessment should compare promised and delivered employment, service provision, compensation, local procurement and environmental outcomes. The project register developed by the Secretariat of the China–Pakistan Economic Corridor can set official implementation milestones, but independent evidence of performance and the level of community development must be gathered for conclusions on equitable development (China–Pakistan Economic Corridor Secretariat). The takeaway is to prioritize asset security and make it public and create community benefit, not consider them mutually exclusive.

Policy Framework: From Threat Management to Resilience

There is a need for differentiated time horizons and a clear institutional assignment in a sustainable response. The short-term objective is to maintain the life and essential services; the medium-term objective is to minimize governance and economic vulnerabilities; and the long-term objective is to create institutions that can adjust to the changing threats. This whole of government should not be about administrative centralisation, and whole of society should avoid civic centralisation and legitimate political disagreement.

First, create a provincial risk assessment process, which is shared and regulated by law, and includes relevant provincial departments, civilian law enforcement, federal security authorities, local authorities and infrastructure

operators. Its output should distinguish confirmed events, assessed threats and unattributed allegations. Risk registers should identify vulnerable assets and affected populations, clearly allocating incident response, prosecution, service restoration and public communication responsibilities. Information sharing should be proportionate, audited and subject to applicable privacy and legal requirements. The central performance measure is not the number of coordination meetings but whether response times, investigations and public safety improve.

Second, prioritize governance legitimacy. Strengthen local-government service responsibilities and grievance mechanisms; publish district-level commitments and progress for water, health, education and roads; and require transparent consultation on major resource and infrastructure decisions. Distributive issues should be raised in federal–provincial discussions in an accountable way of budgetary and administrative processes. Independent complaints mechanisms are especially valuable in cases of citizens' allegations of wrongdoing. There can be less abuse and less wrongful "trade-off" between security and rights when there are rule-of-law protections. Political inclusion is a form of security investment; it is better able to collect, pool and resolve information and disagreements before they escalate.

Third, take a very local benefit approach related to CPEC projects and mineral projects. Project agreements should outline recruitment and training measures, opportunities for locally sourced materials, environmental reporting, and easy tools for addressing compensation issues. Public dashboards should differentiate infrastructure completed, services actually delivered and longer-term development outcomes. Freight and port indicators need to be looked at in the context of the water, health and vocational projects in Gwadar with community feedback and independent verification. Vulnerable routes and installations still require physical safeguards, but investing only in perimeter security cannot generate durable local ownership.

Fourth, start to execute national cyber policy in a provincial level based on risk. Identify critical public-sector and contractor-operated information systems; enforce baseline access controls, backups, patching, staff training and incident reporting; and conduct recovery scenarios for communication outages and/or data breaches. Implement a clear national incident-response mechanism and telecom and energy operator liaison. An independent technical review should precede public attribution of cyber incidents. The policy's proposed national, sectoral and organizational tiers provide an existing institutional template rather than requiring an entirely new structure (MoITT, 2021).

Fifth, don't spend money on spurious counter-narrative work. A civilian-led communication protocol should provide timely confirmed facts after attacks, communicate uncertainties, correct mistakes and distinguish unverified claims from deliberate manipulation. Partnerships with journalists, universities and community organizations can improve media literacy while safeguarding legitimate scrutiny. Messages embedded in locally-used languages; and connected to visible administrative responses. NATO's information-threat guidance emphasizes the intentional and coordinated character of harmful manipulation; this standard can help avoid conflating criticism with hostile activity (NATO, 2024).

Sixth, enhance diplomatic and border relations in a carefully targeted and measurable way. Joint procedures for reporting trafficking, reciprocal requests for evidence and dispute de-escalation are more credible than broad accusations unsupported by independently verifiable records. Economic development of provinces should be aligned with lawful cross-border trade and maritime connectivity, as long as the conditions are right. These measures cannot remove regional rivalry, but they can lower incentives for criminal exploitation and improve the capacity to manage incidents before they escalate.

Finally, Indicators should encompass civilian casualties, violence, case resolving performance, length of service disruptions, school/health clinic accessibility, local procurement, employment outcomes, community complaint resolution, and cyber recovery drills and

independent perceptions of institutional trust. Indicators need baselines at the provincial level, disaggregation by district and regular publication. This annual review should be open admission of unsuccessful interventions and the reallocation of resources. Resilience is not about being invulnerable, it's about being less vulnerable and recovering quicker; it's about not saying that every setback is an enemy success, which is untestable.

Conclusion

Balochistan's security environment since 2001 reflects the intersection of enduring political and socioeconomic grievances with armed violence, cross-border uncertainty and expanding infrastructure and digital exposure. Hybrid-warfare theory is valuable for identifying cases where intentional actors combine instruments to compound their effects, but loses explanatory power when applied indiscriminately to all unrest or governmental shortcomings. Securitization theory clarifies how threat framing shapes policy choices, and resilience supplies a more durable benchmark of success: legitimate institutions, protected services, informed citizens and adaptive coordination. The most defensible strategy for Pakistan is therefore neither exclusively coercive nor exclusively developmental. Intelligence-led protection, lawful accountability, provincial and local participation, equitable economic opportunities, credible information, cybersecurity and diplomatic engagement must work as complementary functions. Public evidence supports the urgency of these measures; it does not support attributing every local grievance or digital disturbance to a unified external operation. An evidence-sensitive, rights-respecting national resilience framework offers a stronger basis for protecting Balochistan's people, sustaining strategic infrastructure and strengthening Pakistan's wider national security.

References

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers. https://doi.org/10.1515/9781685853808

China–Pakistan Economic Corridor Secretariat. (n.d.). Gwadar projects under CPEC. Government of Pakistan. https://cpec.gov.pk/gwadar

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Ministry of Information Technology and Telecommunication. (2021). National cyber security policy 2021. Government of Pakistan. https://pkcert.gov.pk/uploads/2023/06/2021-National-Cyber-Security-Policy-Final.pdf

National Security Division. (2022). National security policy of Pakistan 2022–2026. Government of Pakistan. https://nsd.gov.pk/PublicationDetail/NGE2ZDY0Y2UtODM4Yy00YWE5LTg0NTMtYzQ4OGY2OThkOTBi

North Atlantic Treaty Organization. (2024, October 18). NATO's approach to counter information threats. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats

North Atlantic Treaty Organization. (2026, January 29). Countering hybrid threats. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

Pakistan Bureau of Statistics. (2025). Provincial census report: Balochistan (7th Population and Housing Census–2023). Government of Pakistan. https://www.pbs.gov.pk/sites/default/files/population/2023/reports/Provincial%20Census%20Report%202023-Balochistan.pdf

Pak Institute for Peace Studies. (2026). Pakistan security report 2025. https://pakpips.com/web/wp-content/uploads/2026/02/PIPS%20Security%20Report%2025.pdf

United Nations Development Programme. (2024). Doing digital for development: Access, adopt, anticipate, accelerate (Pakistan National Human Development Report 2023/2024). https://www.undp.org/pakistan/NHDR-2024

IEER
Institute for Excellence in Education & Research