

DOI: [https://doi.org/10.71317/kjard.2.8\(s\).2026.556](https://doi.org/10.71317/kjard.2.8(s).2026.556)

The Kashmir Journal of Academic Research and Development

Journal homepage: <https://rjsaonline.org/index.php/KJARD>

Hybrid Warfare and U.S. Strategic Preparedness: Strategic Challenges, Policy Responses, and Operational Imperatives

Asif Samad (Retd.)

Group Captain Former Faculty, PAF Air War College Institute, Faisal Town, Karachi, Pakistan, Air Force; Independent Hybrid Warfare Researcher & Strategic Analyst

Email: asifsamad761@gmail.com

ARTICLE INFO	ABSTRACT
Received: May 10, 2026 Revised: June 18, 2026 Accepted: June 25, 2026 Available Online: August 21, 2026 Keywords: <i>Hybrid Warfare, U.S. National Defense Strategy, Grey Zone Conflict, Integrated Deterrence, SHADOW Act, Strategic Competition, Resilience</i> Corresponding Author: Asif Samad (Retd.) Email: asifsamad761@gmail.com	This research article examines the evolution of hybrid warfare as a strategic challenge to U.S. national security and analyzes the policy and operational responses articulated in recent U.S. strategic documents and legislative initiatives. The study employs qualitative analysis of primary sources including the 2026 U.S. National Defense Strategy, the National Security Strategy, and the Strategic Hybrid Activities Defense and Operations for the West (SHADOW) Act (H.R. 7632). The research identifies a fundamental tension in U.S. strategy: the prioritization of great power competition and homeland defense creates a "transition window" of vulnerability that adversaries may exploit through hybrid means below the threshold of armed conflict. The article proposes an integrated operational framework for hybrid threat assessment and response, drawing on historical precedents and contemporary strategic analysis. Findings suggest that U.S. hybrid warfare policy must address four critical gaps: attribution ambiguity, decision compression under AI-enabled threats, interagency coordination, and allied resilience capacity. The research concludes that effective counter-hybrid operations require a shift from reactive to proactive resilience-building and from unilateral to coordinated allied engagement.

Introduction

The contemporary strategic environment is characterized by the convergence of traditional and non-traditional threats that challenge the foundational assumptions of U.S. defense planning. Hybrid warfare, defined as the use of a combination of military and non-military, covert and overt means to influence, destabilize, or undermine interests—has become an increasingly important feature of strategic competition among major powers. The 2026 U.S. National Defense Strategy acknowledges this reality, yet the important challenges remain in integrating operational and policy response to hybrid threats.

The central problem confronting U.S. decision-makers is: how to make timely and effective decisions when confronted with integrated, multi-domain threats that deliberately obscure attribution, compress decision timelines, and create ambiguity about escalation consequences. This problem is exacerbated by strategic choices that prioritize great power competition while potentially creating exploitable vulnerabilities in the "grey zone" between peace and war.

Research Questions

This study addresses the following research questions:

1. **RQ1:** How does the 2026 U.S. National Defense Strategy conceptualize and address hybrid warfare threats, and what are the strategic implications of this conceptualization?
2. **RQ2:** What institutional and policy mechanisms is the U.S. government developing to counter hybrid threats, as evidenced by legislative initiatives such as the SHADOW Act?
3. **RQ3:** What are the critical operational gaps in current U.S. hybrid threat preparedness, and how can these gaps be addressed through enhanced analytical frameworks and allied cooperation?
4. **RQ4:** How can the U.S. balance the competing demands of great power competition, homeland defense, and allied security commitments while maintaining effective hybrid threat deterrence?

Hypotheses

1. **H1:** The prioritization of homeland defense and conventional deterrence within broader strategic competition may create gaps in preparedness for persistent hybrid activities conducted below the threshold of armed conflict.
2. **H2:** Legislative initiatives such as the SHADOW Act represent an emerging institutional recognition of hybrid threats but lack the operational integration and allied coordination mechanisms necessary for effective counter-hybrid operations.
3. **H3:** The operational gap in hybrid threat response is primarily a function of analytical fragmentation across disciplinary silos, which adversaries exploit by designing campaigns that straddle cyber, information, economic, and military domains.
4. **H4:** Enhanced allied resilience—particularly in logistics, energy, and cyber defense—can provide a more sustainable long-term response to hybrid threats than reactive military or diplomatic measures alone.

Hypothesis Testing Approach

The hypotheses will be tested through qualitative analysis of primary documents (the 2026 National Defense Strategy, the SHADOW Act, and related policy statements), secondary literature on hybrid warfare, and case analysis of contemporary hybrid operations. The analysis employs a structured analytical framework adapted from operational decision-making to assess the coherence and effectiveness of U.S. hybrid warfare policy.

Literature Review

The Evolution of the Hybrid Warfare Concept

The concept of hybrid warfare has evolved significantly since its emergence in the strategic literature following the 2006 Lebanon War. As Stefanachi (2024) documents, the term "hybrid war" was initially coined to signal the advent of a novel kind of armed conflict characterized by an unprecedented amalgam of regular and irregular components. Against the backdrop of the "color revolutions" and subsequently the Russian annexation of Crimea and its intervention in Donbass, the notion has been employed both in Russia and Western countries primarily to refer to an array of fundamentally non-military (and mostly subversive) strategies that blur the distinction between peace and war.

Çetinkaya (2025) notes that hybrid warfare is "a multifaceted and dynamic form of conflict that employs a combination of both traditional and modern warfare methods," not limited to inter-state conflicts but executable by non-state actors, terrorist organizations, cyber aggressors, and even individuals. This broad conceptualization presents definitional challenges that have complicated both scholarship and policy formulation.

Recent scholarly work has sought to systematize the hybrid warfare concept. Korean researchers (2026) periodize the evolution into a formative phase (2007–2013) and a post-Crimean expansionary phase (2014–2021), identifying three key criteria for analysis: core issues, executing actors, and the scope of means. This scholarship criticizes the absence of causal mechanisms, the politicization of the concept, and the marginalization of physical means in some accounts, proposing a redefinition that restores the significance of conventional and physical strike capabilities.

The strategic interests of the United States are inextricably linked to the challenge of hybrid warfare, as contemporary scholarship emphasizes that threats operating below the threshold of armed conflict fundamentally undermine traditional deterrence and defense paradigms. Hoffman (2007) observed that hybrid warfare represents a "blurring of the modes of war" (p. 30), wherein adversaries combine conventional military capabilities with irregular tactics, cyber operations, and information

warfare to achieve strategic objectives without triggering a full-scale military response. This ambiguity in attribution and escalation dynamics directly threatens U.S. national security interests, particularly as adversaries exploit the "grey zone" between peace and war to erode American influence, destabilize allied nations, and test the credibility of U.S. commitments (Mazarr et al., 2019). The challenge is compounded by the fact that such campaigns often unfold over extended time horizons, making them difficult to detect, attribute, and counter using traditional intelligence and defense frameworks, thereby requiring a fundamental rethinking of how the United States protects its global interests in an era of strategic competition (Radin, 2020).

The prioritization of great power competition and conventional deterrence, while strategically appropriate, may inadvertently create exploitable vulnerabilities that adversaries can leverage through persistent hybrid activities below the armed conflict threshold. Recent analyses of U.S. strategy suggest that the emphasis on peer conflict readiness has diverted attention and resources from the full spectrum of grey zone threats, leaving critical gaps in homeland defense and allied security cooperation (Brands, 2022). This concern is empirically supported by the Ukraine case, where Russian hybrid campaigns combined cyber-attacks, disinformation, economic coercion, and proxy forces to destabilize the target state while remaining below the threshold that would trigger NATO's collective defense provisions (Galeotti, 2019; Snyder, 2020). For the United States, the strategic implications are profound, as adversaries increasingly view hybrid warfare as a cost-effective means to achieve geopolitical objectives while avoiding the risks of direct military confrontation, thereby challenging the foundational assumptions of U.S. deterrence theory and necessitating a more comprehensive approach to protecting allied resilience in logistics, energy infrastructure, and cyber defense (Cordesman, 2017).

Zahid (2020) explained that at last effective counterstrike forced Soviet Union to withdrawal from Afghanistan, Pakistan, Afghanistan, and United States signed the Geneva Accords with the Soviet Union, which opened the way of peaceful resolution of the Afghanistan problem. However, it is a continuous challenging area for US in the South Asian region.

In response to these challenges, U.S. policy and institutional mechanisms are evolving to recognize hybrid threats, yet critical gaps remain in operational integration and allied coordination that undermine effective counter-hybrid operations. The scholarly literature consistently identifies interagency fragmentation and insufficient coordination with allies as primary obstacles to effective hybrid threat response, as hybrid campaigns are inherently multi-domain and require synchronized action across diplomatic, informational, military, and economic instruments of national power (Fridman, 2018; Radin, 2020). Legislative initiatives such as the SHADOW Act represent an emerging institutional recognition of these threats, but current frameworks lack the analytical integration and operational agility necessary to counter adversaries who deliberately design campaigns that straddle cyber, information, economic, and military domains (Mazarr et al., 2019).

To effectively protect U.S. interests, scholars increasingly advocate for a shift from reactive to proactive resilience-building, emphasizing enhanced allied cooperation, improved attribution capabilities, and the development of decision-support tools that can function under the compressed timelines characteristic of AI-enabled hybrid threats (Brands, 2022; Snyder, 2020). Ultimately, the long-term defense of U.S. strategic interests requires moving beyond unilateral actions toward a coordinated, resilient alliance network capable of deterring and responding to the multifaceted nature of hybrid warfare.

Historical Antecedents: The *Dau Tranh* Synthesis

Contemporary hybrid warfare has significant historical antecedents that provide analytical insight. The Vietnamese communist strategy of *dau tranh* during the Vietnam War exemplified an integrated approach combining armed conflict, political warfare, and diplomatic struggle. As documented by the U.S. Army War College, the North Vietnamese "totally integrated two principal forms of force, armed conflict and political conflict," creating "a war waged on several fronts, not geographical fronts, but programmatic fronts, all conducted by one authority, all carefully meshed to serve one end, the seizure of national power".

This historical precedent reveals the fundamental logic of hybrid warfare: the integration of military and non-military means toward political objectives, with the psychological and political dimensions often taking precedence over purely military outcomes. The Vietnamese experience also demonstrates the importance of targeting adversary public opinion as a primary vulnerability, a lesson that contemporary hybrid warfare practitioners have adapted to the digital information environment.

Contemporary Hybrid Threat Vectors

The academic literature identifies multiple vectors of hybrid warfare that are relevant to U.S. strategic planning:

Cyber Operations: As Arquilla and Ronfeldt (1993) presciently argued, "cyberwar is coming," and contemporary scholarship has extensively documented the role of cyber capabilities in hybrid campaigns. The Stuxnet case exemplifies the limits and possibilities of cyber warfare, suggesting that cyber capabilities "can marginally enhance the power of stronger over weaker actors" while also demonstrating the complexity of weaponization and the feasibility of defense.

Information Warfare and Cognitive Operations. Contemporary hybrid warfare places increasing emphasis on information operations and attempts to influence the cognitive environment. The SHADOW Act expressly identifies information campaigns targeting United States interests as one form of hybrid warfare activity, reflecting institutional recognition of the informational dimension of hybrid competition.

Economic Coercion: Economic sanctions and economic pressure have become increasingly prominent hybrid warfare tools. Pape's (1997) analysis of economic sanctions argues that they "do not work" in the sense of achieving political objectives, yet contemporary practitioners continue to employ economic coercion as a hybrid instrument. The weaponization of migration flows, identified in the SHADOW Act, represents a newer form of hybrid economic-political pressure.

Proxy Warfare and Irregular Forces: Mumford's (2013) analysis of proxy warfare identifies it as a "significant feature of the character of conflict in the future". The SHADOW Act explicitly includes "deployment of operatives, irregular armed groups, and uses of regular forces in ways that threaten United States or allied interests" within the definition of hybrid warfare activities.

U.S. Strategic Interests and Hybrid Threats in South Asia

The strategic challenges the United States faces in South Asia are deeply intertwined with the region's volatile security landscape, which is characterized by intensifying great power competition, persistent transnational terrorism, and the proliferation of hybrid warfare tactics among regional actors. U.S. strategic interests in South Asia are defined by three principal objectives—geopolitical, economic, and counterterrorism—all of which are increasingly threatened by hybrid campaigns that operate below the threshold of conventional armed conflict (Stimson Center, 2024). The geopolitical imperative requires Washington to prevent any single hegemonic power, particularly China, from dominating the region, while the economic interest centers on securing access to critical mineral reserves in Pakistan's western provinces, including the Reko Diq deposit, which holds an estimated 5.9 billion tons of ore containing copper and gold vital to modern technology and the energy transition (The Express Tribune, 2026). Counterterrorism remains a paramount concern, as Afghanistan remains a haven for more than twenty terrorist and militant groups, with violence capable of spilling across borders and threatening international security, prompting the U.S. to maintain security cooperation with Pakistan, which senior U.S. officials have described as "another important partner in the region" (The Friday Times, 2026).

Regional Competition and U.S. Policy Responses

The region's hybrid warfare challenge is further complicated by the strategic competition between India and Pakistan, where adversarial states employ non-military and irregular means to achieve political objectives without triggering escalation to conventional warfare. Strategic experts have warned that future conflicts in South Asia will increasingly involve "hybrid warfare, cyber capabilities and narrative warfare" alongside conventional military means, as India seeks to normalize limited warfare under nuclear conditions and exploit compressed decision-making timelines (Herr, 2026). Analysts have characterized India's approach as a comprehensive hybrid strategy designed to damage, demoralize, and destabilize Pakistan through backing separatist groups, exacerbating ethnic and sectarian tensions, and conducting information operations to isolate Pakistan internationally (Shahid, 2026). This dynamic poses a direct challenge to U.S. interests, as proxy warfare and hybrid campaigns in the region threaten the stability of allied partners and complicate Washington's efforts to balance its relationships with both India and Pakistan while maintaining strategic influence (Azad et al., 2023). Pakistani strategic planners have emphasized the need for adaptive deterrence that integrates nuclear, conventional, and grey-zone capabilities, as well as "cognitive resilience" to counter the effects of disinformation and narrative manipulation that accompany hybrid operations (Centre for Development and Stability, 2026).

For the United States, addressing hybrid warfare challenges in South Asia requires a comprehensive approach that strengthens allied resilience, enhances intelligence coordination, and navigates the complex web of regional rivalries without provoking escalation. The absence of a unified conceptual framework for countering hybrid and irregular warfare across the Indo-Pacific region, as identified by the Irregular Warfare Center, represents a critical gap that the U.S. must address, particularly given Pakistan's extensive experience with unconventional warfare, counterinsurgency, and counterterrorism—the three main pillars of U.S. irregular warfare doctrine (Defense Strategies Institute, 2026; Irregular Warfare Center, 2026). Emerging U.S.-Pakistan security cooperation, including ongoing counterterrorism dialogue and joint exercises, suggests a renewed recognition of Pakistan's strategic importance, yet Washington must also contend with competing Chinese influence in the region, as Beijing seeks to protect its Belt and Road Initiative investments and maintain its strategic partnership with Islamabad (Chacko, 2026; Basnyat, 2026). The challenge for U.S. policymakers is to craft a South Asia strategy that leverages regional partnerships to counter hybrid threats, ensures the stability of nuclear-armed rivals, and prevents the region from becoming a theater for unchecked great power competition, all while maintaining the credibility of U.S. commitments to allied security and deterrence (Check & Fisher, 2022).

Integrated Deterrence and the U.S. Strategic Response

The U.S. strategic response to hybrid threats is articulated through the concept of "integrated deterrence." "Goswami (2024), writing for the Indian Council of World Affairs, explains that integrated deterrence "talks about integrating all instruments of power, including strategic deterrence, under a coordinated military modernization plan at strategic and conventional levels to deter potential adversaries during a limited and non-nuclear strategic attack".

Goswami's analysis also discusses Conventional-Nuclear Integration as part of the broader integrated-deterrence approach, including efforts to strengthen alliances and partnerships across the Indo-Pacific, Europe, and West Asia. This approach seeks to achieve deterrence through denial, resilience, cost imposition, and escalation management. However, scholars have expressed concerns about the effectiveness of integrated deterrence against coordinated adversaries, suggesting that success "hinges not only on collaboration with existing allies and partners but also acquiring new ones and making the ties among them stronger".

The Brookings Institution (2026) emphasizes that "resilience as deterrence" should be a practical implication of U.S. strategy, requiring a focused program of security cooperation that helps allies and partners build the resilience needed to operate under attack. This includes hardening physical infrastructure and the digital systems that run them, treating "cyber and resilience as a single integrated problem".

Methodology

Research Design

This study employs a qualitative research design appropriate for analyzing complex policy and strategic documents. The approach is interpretive and analytical, seeking to understand the meaning, implications, and coherence of U.S. hybrid warfare policy through systematic examination of primary and secondary sources.

Data Sources

Primary data sources include:

- **The 2026 U.S. National Defense Strategy:** Analyzed for its conceptualization of hybrid threats, strategic priorities, and resource allocation implications.
- **The 2025 U.S. National Security Strategy:** Examined for the broader strategic framework that informs defense policy.
- **H.R. 7632, the SHADOW Act:** Analyzed for legislative responses to hybrid threats, institutional mechanisms proposed, and definitions of hybrid warfare activities.
- **Congressional Budget Office Analysis of H.R. 7632:** Examined for fiscal implications and implementation expectations.

Secondary data sources include scholarly literature on hybrid warfare, policy analysis from institutions such as the Brookings Institution, and selected contemporary analyses used to examine emerging hybrid-threat developments.

Analytical Framework

The analysis employs a structured analytical framework adapted from the Hybrid Threat Operational Preparedness Framework (HTOPF) proposed in the policy document accompanying this research. The framework establishes a systematic analytical chain:

Threat → Indicator → Vulnerability → Operational Effect → Decision Risk → Escalation Risk → Resilience Measure → Response Option

The contribution of HTOPF lies primarily in integration rather than in claiming an entirely new set of security concepts. Threat analysis, vulnerability assessment, resilience, escalation management, and response planning already exist as established areas of study and practice. The framework brings these elements into a single analytical sequence intended to help analyst move from the observation of a hybrid indicator to an assessment of its operational and decision-making consequences.

This framework enables systematic assessment of how U.S. policy addresses each stage of the hybrid threat response cycle and identification of gaps in current approaches.

Although the study relies on open-source documentary analysis, the structure of the analytical framework is also informed by the author's professional experience in time-sensitive air defence decision environments, command and control, strategic military education, and subsequent research on hybrid warfare. These experiences are not treated as empirical evidence themselves. Rather, they inform the framework's emphasis on threat detection, decision risk, escalation assessment, resilience, and response under conditions of uncertainty.

Limitations

This study is limited by the recency of the documents analyzed and the evolving nature of the hybrid threat environment. Additionally, classified aspects of U.S. strategy and intelligence assessments are not available for analysis, potentially limiting the comprehensiveness of findings.

The HTOFP should therefore be understood as an analytical framework requiring further testing and refinement rather than as a validated operational model. Future research could apply the framework to additional case studies and assess the utility through expert review, tabletop exercises, professional military education, or other structured analytical settings.

Analysis

The 2026 National Defense Strategy: Strategic Choices and Hybrid Threat Implications

The 2026 National Defense Strategy represents a significant strategic reorientation of U.S. defense priorities. The strategy's central choice is to prioritize "defending the U.S. Homeland and deterring China" while requiring allies to take "primary responsibility for Europe's conventional defense, with critical but more limited U.S. support". This represents a fundamental redistribution of risk within the alliance system.

The Threat Perception Gap

The 2026 NDS describes Russia as a 'persistent but manageable threat' and places greater responsibility on European allies for conventional defense. One contemporary analysis interprets this strategic distinction as creating a potential 'threat perception gap' in the grey zone, where sabotage, cyber activity, and other below-threshold actions may not generate the same response as conventional aggression.

This strategic choice creates conditions that adversaries can exploit. As one analysis notes, the NDS "creates an environment for Moscow to test NATO's cohesion through 'accidents' and 'incidents' that force mobilization without ever crossing the Article 5 threshold". The separation of "full-scale invasion" from "grey zone" operations creates ambiguity that adversaries can manipulate.

The Transition Window Problem

The strategy's implementation creates what analysts describe as a "transition window" of vulnerability. The assumption that NATO and South Korea can take "primary responsibility for regional defense within acceptable timeframes" confronts daunting barriers: European debt levels limit defense spending, indigenous production of precision munitions remains limited, and untested casualty tolerance raises questions about political sustainability.

This may create transitional period of vulnerability during which adversaries could seek to exploit gaps between changing U.S. commitments and the development of allied capabilities. As Military Times analysis observes, "Britain's 1937 Imperial Defence White Paper articulated clear priorities, but this didn't prevent Germany from exploiting the transition period before Allied rearmament". Adversaries will likely exploit similar vulnerabilities during the U.S. strategic transition.

The Tactical-Strategic Disconnect

The recent Operation Absolute Resolve in Venezuela provides a useful case through which to examine the distinction between tactical operation success and longer-term strategic effects. The operation demonstrated substantial U.S. power projection capability, while subsequent political and security conditions raise broader questions concerning the relationship between immediate operational outcomes and enduring strategic effects.

This disconnect between tactical capability and strategic outcome is directly relevant to hybrid warfare. Hybrid operations typically achieve strategic effects through accumulation of tactical actions below the threshold that would trigger decisive U.S. military response. The U.S. can strike anywhere but cannot effectively counter the sustained, ambiguous operations that characterize hybrid campaigns. (Zahid, 2026)

The SHADOW Act: Institutional Response to Hybrid Threats

The Strategic Hybrid Activities Defense and Operations for the West Act (H.R. 7632) represents a significant congressional response to hybrid-warfare concerns in the 119th Congress. The Congressional Budget Office estimates implementation costs at less than \$500,000 annually and total \$1 million over the 2026-2031 period.

Institutional Framework

The SHADOW Act establishes a Coordinator for Hybrid Warfare Accountability within the Department of State, reporting to the Under Secretary for Political Affairs. The Coordinator's responsibilities include:

1. Assessing, integrating, and disseminating information on hybrid warfare activities, including Chinese and Russian-linked efforts
2. Identifying analytic and operational gaps in U.S. understanding of hybrid threats
3. Coordinating within NATO and with other key partners for timely information sharing
4. Supporting resilience and de-risking efforts with allies and partners

Definition of Hybrid Warfare Activities

The SHADOW Act provides a comprehensive definition of hybrid warfare activities that includes:

- Information campaigns targeting U.S. interests
- Cyber-attacks
- Economic pressure, coercion, or manipulation
- Deployment of operatives, irregular armed groups, and regular forces
- Weaponization of migration flows
- Sabotage of critical infrastructure
- Targeted assassinations or attempted assassinations

This definition is significant for providing a common operational vocabulary and analytical framework, addressing the SHADOW Act's explicit goal of "common definitions for gray zone activities, to strengthen shared understanding, preparedness, and mitigation efforts".

Implementation Considerations

Several limitations in the SHADOW Act deserve attention. First, the designation of a senior official "from among existing officers or employees" rather than as a new position may limit the Coordinator's authority and visibility. Second, the reporting requirement—a strategy within 60 days and annual reports for three years—creates bureaucratic reporting mechanisms but does not establish operational response capabilities. Third, the focus on diplomatic coordination, while valuable, does not address the operational integration of cyber, information, economic, and military response capabilities.

Operational Gaps in Hybrid Threat Response

Analysis of U.S. hybrid warfare policy reveals four critical operational gaps:

Attribution Ambiguity

Hybrid operations are designed to create plausible deniability, complicating response decisions. The SHADOW Act's focus on "common attribution language" acknowledges this challenge but does not resolve it. Recent analysis of the U.S.–Iran confrontation illustrates how proxy activity, cyber operations, economic coercion, and periodic military escalation can sustain competition in the grey zone even when overt hostilities temporarily subside. Attribution ambiguity can constrain timely decision-making because uncertainty over responsibility increases the risk of misattribution, disproportionate response, or unintended escalation.

Decision Compression Under AI-Enabled Threats

AI technologies accelerate hybrid operations across multiple dimensions: collection, targeting, synthetic information production, and decision support. The 2026 NDS provides limited detail on how AI-enabled decision compression may affect hybrid threat response and escalation management. As noted in the accompanying policy document, "a tactical/non-kinetic event can generate strategic consequences" before decision-makers can adequately respond, creating dangerous escalation dynamics.

Interagency Coordination

Hybrid threats require coordinated responses across government agencies. The SHADOW Act attempts to address this through the Coordinator position but does not establish mechanisms for operational integration across the Departments of State, Defense, Energy, and the intelligence community. The Brookings Institution emphasizes that "cyber and resilience" must be treated "as a single integrated problem," requiring levels of coordination that existing structures may not fully support.

Allied Resilience Capacity

The NDS places greater responsibility on allies or regional defense, while important capability gap remains in the areas such as logistic, energy resilience, cyber defense, and continuity under hybrid pressure. As Brookings analysis notes, "deterrence becomes brittle when it depends on a rapid timeline but rests on fragile infrastructure and untested cross-border procedures". The SHADOW Act's provision for "supporting resilience and de-risking efforts with allies and partners" acknowledges this gap but does not specify the resources or mechanisms for addressing it.

Historical Lessons and Contemporary Application

The historical precedent of the *dau tranh* strategy in Vietnam offers enduring lessons for contemporary hybrid warfare. Hanoi's approach demonstrated that "moral forces are not only as important as material forces but are inseparable". The Vietnamese communists understood that the main front in their war was not in Southeast Asia but in the United States—targeting American public opinion as the decisive vulnerability.

Contemporary adversaries apply similar logic, targeting the cognitive dimension of conflict through information operations, disinformation, and AI-enabled synthetic media. The 2026 NDS and SHADOW Act implicitly acknowledge this threat but do not fully address the cognitive dimension of hybrid warfare.

Cross Theater Relevance and The South Asian Security Environment

The analytical problem examined in this study are not limited to the European security environment. South Asia provides another important setting in which conventional deterrence, nuclear risk, information operations, emerging technologies, proxy dynamics, and great-power competition interact. The author's earlier research on Hybrid Warfare and AI-Enabled escalation in South Asia suggests that attribution ambiguity, compressed decision timelines, and escalation uncertainty can take different forms across regional environments. This reinforces the value of an analytical framework that can be adapted to different strategic contexts rather than being tied to a single theater.

Findings

Hypothesis Testing Results

H1: Evidence Consistent with a Threat Perception Gap

Analysis of the 2026 National Defense Strategy confirms that the prioritization of great power competition and homeland defense creates a dangerous "threat perception gap" regarding hybrid warfare. By categorizing Russia as "manageable" and delegating grey zone operations to regional allies, the U.S. creates conditions that adversaries can exploit. The evidence reviewed provides support for H1.

H2: Institutional Recognition with Operational Gaps

The SHADOW Act represents significant institutional recognition of hybrid threats, establishing a Coordinator position and requiring comprehensive reporting. However, the act does not establish operational integration mechanisms, resource allocations for resilience building, or response authorities. The evidence reviewed supports H2's proposition of institutional recognition accompanied by operational limitations.

H3: Evidence of Analytical Fragmentation

Analysis of U.S. hybrid threat response confirms that analytical fragmentation across disciplinary silos remains a critical vulnerability. The SHADOW Act's focus on "common definitions for gray zone activities" addresses this gap at the conceptual level but does not establish integrated analytical architectures. The evidence reviewed provides support for H3.

H4: Evidence Supporting Resilience as a Long-Term Response

The analysis supports the proposition that enhanced allied resilience is the most effective long-term response to hybrid threats. However, U.S. policy documents do not adequately address the resource requirements, coordination mechanisms, or timeline for building allied resilience. The findings provide partial support for H4 while also identifying significant implementation and resource questions.

Key Findings

1. **Strategic Reorientation May Create Transitional Vulnerabilities:** Changes in U.S. strategic priorities may create periods during which adversaries seek to exploit gaps between changing U.S. commitments and developing allied capabilities.
2. **Institutional Recognition Outpaces Operational Capability:** The SHADOW Act establishes important institutional frameworks for hybrid threat coordination but does not address operational integration, resource allocation, or response authorities.
3. **Allied Resilience Gap:** Important capability gaps remain in allied logistics, energy resilience, and cyber defense, while current policy documents provide limited detail on how these gaps will be addressed.
4. **Cognitive Dimension Underappreciated:** The policy documents examined in this study provide less detailed treatment of the cognitive dimension of Hybrid warfare than of several other security challenges. U.S. hybrid warfare policy focuses primarily on cyber and conventional threats, with less attention to the cognitive dimension of hybrid warfare that targets decision-making.
5. **Historical Lessons Not Applied:** The historical experience of integrated warfare strategies offers important lessons for contemporary hybrid threats, yet the policy documents examined provide limited explicit discussions of how these historical lessons might inform contemporary hybrid-threat preparedness.

Recommendations

Policy Recommendations

Recommendation 1: Establish a Comprehensive Hybrid Warfare Doctrine

The U.S. should develop comprehensive hybrid warfare doctrine that addresses offense, defense, and resilience across all relevant domains. This doctrine should integrate historical lessons from integrated warfare strategies and contemporary analysis of AI-enabled threats. The doctrine should establish clear decision-making authorities, attribution thresholds, and response parameters for hybrid contingencies.

Recommendation 2: Enhance Interagency Integration

The Coordinator established by the SHADOW Act should be supported by a formal interagency hybrid threat coordination mechanism that includes the Departments of State, Defense, Energy, and Homeland Security, as well as the intelligence community. This mechanism should conduct joint planning for hybrid contingencies and coordinate resource allocation across agencies.

Recommendation 3: Prioritize Allied Resilience Investment

The U.S. should establish a dedicated program for allied resilience building, including funding for infrastructure hardening, cyber defense, logistics, and energy security. This program should treat "cyber and resilience as a single integrated problem" and prioritize the critical nodes that determine operational continuity.

Recommendation 4: Develop AI-Enabled Hybrid Threat Assessment Capabilities

The U.S. should invest in AI-enabled detection and analysis capabilities specifically designed for hybrid threat assessment, including cross-domain correlation of cyber, information, economic, and military indicators. These capabilities should support compressed decision timelines while maintaining analytical rigor.

Recommendation 5: Strengthen the Cognitive Dimension of Resilience

The U.S. should develop comprehensive cognitive resilience capabilities, including media literacy programs, strategic communications frameworks, and counter-disinformation operations. These capabilities should address the information and cognitive dimensions of hybrid warfare.

Operational Recommendations

Recommendation 6: Establish Hybrid Threat Operational Monitoring

The Department of Defense should establish dedicated operational monitoring for hybrid threats that integrates cyber, information, economic, political, and military indicators into a unified operational picture. This monitoring should support early detection and rapid response to hybrid operations.

Recommendation 7: Develop Rapid Response Capabilities

Given the compressed decision timelines characteristic of hybrid operations, the U.S. should develop rapid response capabilities specifically designed for hybrid contingencies, including pre-planned or scenario-based response options consistent with applicable authorities and escalation-management considerations, streamlined decision processes, and appropriate crisis-response mechanisms.

Recommendation 8: Conduct Hybrid Threat Exercises and Wargames

The U.S. should conduct regular exercises and wargames that simulate complex hybrid threat scenarios, incorporating compressed decision timelines and attribution ambiguity. These exercises should evaluate decision-making under hybrid pressure and identify capability gaps.

Recommendation 9: Establish Hybrid-Specific Rules of Engagement

U.S. defense and policy communities should examine whether existing authorities, decision protocols, and response guidance adequately address attribution ambiguity, below-threshold activities, and the escalation risks associated with hybrid operations. Where gaps are identified, appropriate guidance and response procedures could be further developed or refined.

Investment Recommendations

Recommendation 10: Human Capital Investment

The U.S. should invest in developing the analytical skills, training, and experience necessary for effective hybrid threat assessment, including recruitment of personnel with relevant skills, comprehensive training programs, and career development paths for hybrid warfare specialists.

Recommendation 11: Resilience Infrastructure Investment

Investment should prioritize resilience infrastructure over perfect prevention, including critical infrastructure hardening, information resilience capabilities, economic resilience, and cognitive resilience development.

Recommendation 12: International Partnership Investment

The U.S. should invest in international partnership capabilities for hybrid threat assessment and response, including intelligence sharing systems, joint analysis capabilities, training programs for partners, and capacity building.

Conclusion

This research has examined the challenge of hybrid warfare to U.S. national security and analyzed the policy and operational responses articulated in the 2026 National Defense Strategy and the SHADOW Act. The findings reveal a fundamental tension in U.S. strategy: the prioritization of great power competition and homeland defense creates a "transition window" of vulnerability that adversaries can exploit through hybrid means below the threshold of armed conflict.

The analysis confirms that current U.S. hybrid warfare policy exhibits institutional recognition of the threat but lacks the operational integration, resource allocation, and allied coordination mechanisms necessary for effective response. Four critical gaps were identified: attribution ambiguity, decision compression under AI-enabled threats, interagency coordination, and allied resilience capacity.

Addressing these gaps requires a comprehensive approach that integrates policy, operational, and investment recommendations. The U.S. must develop comprehensive hybrid warfare doctrine, enhance interagency integration, prioritize allied resilience investment, develop AI-enabled assessment capabilities, and strengthen the cognitive dimension of resilience. Operationally, the U.S. should establish hybrid threat monitoring, develop rapid response capabilities, conduct regular exercises, and develop hybrid-specific rules of engagement.

Hybrid threats are likely to continue evolving as artificial intelligence, information technologies, cyber capabilities, and other instruments become more deeply integrated into strategic competition. The challenge for U.S. policymakers and security institutions is therefore not simply to identify individual hostile activities, but to understand how those activities interact, how they affect decision-making, and how they may generate wider operational or escalation consequences. The HOPF offers one structured approach for organizing that analysis by linking threats and indicators to vulnerabilities, operational effects, decision risks, escalation risks, resilience measures, and response options. Further research and testing should determine how the framework can be refined and adapted across different strategic environments.

Bibliography

- Al Jazeera. (2026, January 19). "In Iran, the US-Israeli addiction to hybrid warfare is on full display." *Al Jazeera Opinion*.
- Bachmann, S.-D., & Gunneriusson, H. (2015). "Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security." *Scientia Militaria: South African Journal of Military Studies*, 43(1), 77-98. <https://doi.org/10.5787/43-1-1110>.
- Berry, R. (2026, January 29). "America can strike anywhere—but can it stay anywhere?" *Military Times*.
- Çetinkaya, Ş. (2025). "Hybrid war: International security at the intersection of traditional and modern warfare." *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi*.
- Clemis, M. G. (2025). "The Enduring Lessons of Vietnam: Implications for US Strategy and Policy." *Parameters*, 55(2), 117-134. <https://doi.org/10.55540/0031-1723.3347>.
- Congressional Budget Office. (2026, April 16). "H.R. 7632, Strategic Hybrid Activities Defense and Operations for the West Act." *Cost Estimate*.
- Dowell, S. (2026, January 26). "Trump's new defense strategy creates space for Russia to wage grey-zone warfare." *TVP World*.
- Eom, G. H., Song, H.-Y., & Kwoun, N. (2026). "The Evolution of Hybrid Warfare and Paths toward Theoretical Systematization." *Korea Journal of Military Affairs*, 19, 51-84. <https://doi.org/10.33528/kjma.2026.6.19.51>.
- Goswami, M. (2024, October 25). "Two Fronts, One Strategy: The US Approach of Integrated Deterrence." *Indian Council of World Affairs*.
- Johnson, R. (2018). "Hybrid War and Its Countermeasures: A Critique of the Literature." *Small Wars & Insurgencies*, 29(1), 141-163. <https://doi.org/10.1080/09592318.2018.1404770>.
- Lindsay, J. R. (2013). "Stuxnet and the Limits of Cyber Warfare." *Security Studies*, 22(3), 365-404. <https://doi.org/10.1080/09636412.2013.816122>.
- Mumford, A. (2013). "Proxy Warfare and the Future of Conflict." *The RUSI Journal*, 158(2), 40-46. <https://doi.org/10.1080/03071847.2013.787733>.
- Nouri, B., & Parmar, I. (2026, June 23). "US-Iran war headed for the gray zone." *Asia Times*.
- Noyes, A., & Humpal, J. R. (2026, August 5). "How to actually share America's defense burden with allies." *Brookings Institution*.
- Pape, R. A. (1997). "Why Economic Sanctions Do Not Work." *International Security*, 22(2), 90-136. <https://doi.org/10.2307/2539368>.
- Rid, T. (2012). "Cyber War Will Not Take Place." *The Journal of Strategic Studies*, 35(1), 5-32. <https://doi.org/10.1080/01402390.2011.608939>.
- Stefanachi, C. (2024). "Guerra ibrida: Origine, significati ed equivoci di un concetto ambiguo." *Storia del Pensiero Politico*, 13(2), 239-264. <https://doi.org/10.4479/114313>.
- The White House. (2025). "National Security Strategy of the United States of America." Washington, DC: The White House.

- Tucker, P. (2026, January 22). "Russian hybrid warfare has become indistinguishable from politics." Defense One.
- U.S. Congress. (2026). "Strategic Hybrid Activities Defense and Operations for the West Act (SHADOW Act)." H.R. 7632, 119th Congress.
- U.S. Department of Defense. (2026). "National Defense Strategy." Washington, DC: U.S. Department of Defense.
- Yaqub, Z., & Shifa, Hassan, "Pakistan and United States Diplomatic Relations Since The May 2025 Indo-Pak War: Role of Soft Power and Digital Diplomacy as Tools of Nation Branding. (2026). *Contemporary Journal of Social Science Review*, 4(2), 171-179. <https://doi.org/10.63878/cjssr.v4i2.2333>
- Shahid, R., Afzal, S., & Yaqub, Z. (2020). Challenges of Militancy and Religious Extremism to National Security of Pakistan: An Analysis. *Pakistan Social Sciences Review*, 4, 403-420.

APPENDIX A: HYBRID THREAT OPERATIONAL PREPAREDNESS FRAMEWORK (HTOPF) SUMMARY

Stage	Analytical Focus	Key Questions
1. Threat Identification	Adversary capabilities	Who can act? What can they do?
2. Indicator Detection	Observable activity	What is happening? What indicators exist?
3. Vulnerability Assessment	System weakness	What could be exploited?
4. Operational Effect Analysis	Consequences	What are the operational implications?
5. Decision Risk Assessment	Decision challenges	What makes decisions difficult?
6. Escalation Risk Assessment	Escalation dynamics	What are the escalation risks?
7. Resilience Measures	Risk mitigation	How can we build resilience?
8. Response Options	Course of action	What can we do in response?

APPENDIX B: GLOSSARY OF KEY TERMS

Attribution Ambiguity: The characteristic of hybrid operations where the source of effects cannot be definitively identified, creating a powerful deterrent effect on response.

Cognitive Resilience: The capacity to sustain effective decision-making under conditions of hybrid pressure, including information warfare and decision compression.

Decision Compression: The acceleration of decision timelines created by AI-enabled operations, which can outpace traditional decision cycles.

Grey Zone: Competitive interactions between state and non-state actors that fall between traditional war and peace duality.

Hybrid Warfare: The use of a combination of military and non-military, covert and overt means to influence, destabilize, or undermine interests.

Integrated Deterrence: The integration of all instruments of power, including strategic deterrence, under a coordinated military modernization plan.

Multi-Domain Convergence: The integration of effects across cyber, information, economic, political, and military domains.

Resilience: The capacity to withstand and recover from hybrid operations rather than simply preventing them.

Strategic Competition: Open-ended situational relationships surrounding varying and evolving interests and the actors' place within the international system.

Transition Window: The period during which the U.S. reduces its regional presence while allies are building their capacity to assume primary responsibility for regional defense.



2026 by the authors; Journal of The Kashmir Journal of Academic Research and Development. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).