



INNOVATIVE RESEARCH THOUGHTS IN SOCIAL SCIENCES

Peer Review, Refereed, Biannual, Multiple Language (Hindi & English), Social Science Journal, Open Access Journal

ISSN: 3107-5096(ONLINE)

VOL. 1, ISSUE 2 (DECEMBER)2025

Beyond Conventional and Asymmetric War: Rethinking Security through Hybrid Warfare

* **Ruby Dabas**

Research Scholar

Department of Political Science

Janta Vedic College, Baraut

Doi: <https://doi.org/10.5281/zenodo.17519743>

PP:61-72

ARTICLE INFO

Received:03-10-2025

Accepted:06-11-2025

Published:01-12-2025

Abstract

The changing face of conflict in the 21st century has blurred the lines between war and peace, state and non-state actors, and soldiers and civilians. The term “hybrid warfare” has emerged to describe these transformations, where conventional military power is fused with irregular tactics, cyber operations, disinformation, and economic coercion. Unlike traditional wars fought on defined battlefields, hybrid warfare exploits ambiguity, leaving targets uncertain about how to respond. This paper explores hybrid warfare as a new security challenge for nation-states, examining its conceptual evolution, identifying its distinctive characteristics and analyzing case studies of Russia in Ukraine, the India-Pakistan dynamic in South Asia, and China’s gray zone operations in the South China Sea. The discussion highlights how hybrid strategies erode sovereignty, undermine democratic institutions, and complicate collective defense. The paper argues that national security must now be reconceptualized beyond conventional and asymmetric frameworks, emphasizing resilience, cross-sectoral defense, and international cooperation.

Keywords: Hybrid Warfare, Security Challenges, Ukraine, South Asia, China, Information Warfare

Introduction:

विविधा युद्धनीतिः स्यात्र ह एको मागः सततं।
यो नु युद्धकुशलो वीरः स भवति पराक्रमवान्॥

This shloka from Mahabharata emphasizes that war strategies are diverse and there is no single approach to achieve victory. In the context of modern hybrid warfare, the lesson is strikingly relevant. Hybrid warfare blends conventional military force with irregular tactics, cyber operations, disinformation campaigns, economic pressure, and proxy actors. Just like the shloka suggests, modern conflicts cannot rely on one fixed method-success depends on adaptability, skill, and tactical intelligence.

Throughout history, the nature of warfare has evolved with the times. In earlier centuries, wars were fought on open fields with identifiable armies and clear territorial goals. The 20th century, shaped by industrial and ideological conflicts, reinforced the dominance of conventional warfare while also bringing insurgencies and guerrilla tactics into prominence, especially during decolonization struggles and the Cold War. These were labeled asymmetric wars because they involved irregular actors challenging state militaries with unconventional

In the 21st century, however, the picture has shifted dramatically. Globalization, digital technologies, and the interconnectedness of economies have created new opportunities for state and non-state actors to pursue conflict without open warfare. Hybrid warfare emerged as a concept to describe this new reality-a method that blends conventional power with cyber attacks, disinformation campaigns, proxy militias, and economic pressure. What makes hybrid warfare particularly difficult is its ambiguity: it sits in the “gray zone,” where adversaries pursue aggressive goals while staying below the threshold of traditional war.

This paper seeks to unpack the concept of hybrid warfare and examine how it challenges traditional ideas of security. It begins with a theoretical overview, traces the evolution of hybrid strategies, and then explores three expanded case studies-Russia in Ukraine, the India-Pakistan conflict in South Asia, and China’s South China Sea strategy. Finally, it reflects on the implications for state sovereignty, democratic governance, and policy responses.

Understanding Hybrid Warfare

The idea of hybrid warfare was popularized in the mid-2000s, especially through the work of military analyst Frank Hoffman. He described hybrid wars as conflicts that combine “conventional capabilities, irregular tactics, terrorism, and criminal disorder” in the same battlespace. What distinguishes hybrid warfare is not merely the presence of these elements but their integration into a coordinated strategy.

Distinctive Features:

Blending of methods: Regular military power is combined with irregular tools like insurgencies or militias.

Multi-domain conflict: Operations extend to cyberspace, information ecosystems, and economic systems.

Plausible deniability: States often hide behind proxies or cyber anonymity, making attribution difficult.

Targeting civilian systems: Civil society, infrastructure, and media are as much targets as military forces.

Incremental escalation: Rather than a declaration of war, adversaries gradually increase pressure.

Hybrid warfare is not entirely new—history shows examples of propaganda, proxy wars, and economic coercion—but the speed, precision, and scale of these operations in the digital age make them uniquely disruptive.

Evolution of Hybrid Strategies

During the Cold War, both the United States and the Soviet Union relied on a mix of proxy conflicts, covert operations, and propaganda. Yet these actions were often overshadowed by the nuclear standoff and the clear distinction between East and West blocs. After the Cold War, globalization and technological innovation provided new tools for states to wage influence. The

attacks of 9/11 and the rise of transnational terrorism demonstrated how irregular actors could use global networks for asymmetric warfare. States studied these methods and began incorporating them into their arsenals.

By the 2010s, hybrid warfare had become a defining feature of global conflict. Russia's seizure of Crimea in 2014, cyber intrusions into Western elections, and China's gray zone maneuvers in maritime disputes all showed how hybrid tactics could achieve strategic goals without triggering outright war.

Case Studies

1. Russia and Ukraine: Hybrid Warfare in Action

The conflict in Ukraine illustrates hybrid warfare more vividly than any other. In 2014, when Russia annexed Crimea, it did not begin with tanks rolling across borders in full view. Instead, it relied on a combination of covert and overt tools: unmarked soldiers known as "little green men" took control of key installations, while local proxies and militias created unrest. At the same time, Russia flooded Ukrainian media with disinformation, portraying the Kyiv government as illegitimate and stirring ethnic tensions.

Cyber attacks also played a role. Ukrainian government websites and infrastructure were targeted, including disruptions to the power grid in 2015 and 2016. These cyber strikes undermined public confidence and demonstrated Russia's reach into the digital domain. Meanwhile, Russia used economic leverage, particularly dependence on natural gas supplies, to pressure Ukraine and its European allies.

The 2022 full-scale invasion was preceded by an intensification of hybrid tactics: disinformation campaigns depicting NATO as an aggressor, cyber intrusions into Western defense networks, and false-flag operations intended to justify Russian military moves. Even during the kinetic war, Russia continues to employ hybrid methods, such as targeting civilian infrastructure, spreading propaganda abroad, and weaponizing energy flows to Europe.

The Ukrainian case reveals the essence of hybrid warfare: a spectrum of actions that weaken the opponent's capacity to resist, both militarily and socially, before and alongside overt combat.

2. South Asia: The India–Pakistan Hybrid Conflict

South Asia offers a different but equally revealing example of hybrid warfare. The relationship between India and Pakistan has long been marked by both conventional wars and cross-border insurgency. In recent decades, however, their rivalry has increasingly adopted hybrid dimensions.

Pakistan has often relied on non-state proxies, particularly militant groups, to carry out attacks in Indian Territory. Events such as the 2008 Mumbai attacks and the 2019 Pulwama bombing illustrate the use of irregular actors to achieve strategic goals while avoiding full-scale war. These attacks blur the line between terrorism and state-sponsored hybrid tactics, as Pakistan maintains plausible deniability.

Cyber operations are also becoming prominent in the India-Pakistan conflict. Both states have accused each other of hacking government websites, financial institutions, and critical infrastructure. Disinformation campaigns on social media, aimed at polarizing domestic opinion or undermining trust in institutions, have also become part of the battlefield.

Military posturing remains in the picture, but hybrid methods allow both sides to exert pressure without escalating into nuclear war—a constant shadow in the region. This hybrid rivalry complicates traditional defense strategies, since responses must address not just border incursions but also online propaganda, cyberattacks, and proxy violence.

3. China and the South China Sea: Gray Zone Strategy

China's approach in the South China Sea demonstrates another form of hybrid warfare, often described as gray zone operations. Rather than direct military conflict, China has pursued incremental territorial expansion using unconventional tools.

Chinese paramilitary vessels, often part of the coast guard or maritime militia, are deployed to harass fishing boats and assert control over disputed waters. Artificial islands have been constructed and militarized, giving China a stronger presence without triggering open hostilities. These actions are supported by legal narratives and propaganda campaigns framing China as a peaceful rising power defending historical rights.

Economic tools also play a central role. China leverages trade and investment to influence smaller states in Southeast Asia, discouraging them from aligning too closely with rival powers. At the same time, information campaigns seek to delegitimize external involvement, particularly by the United States and its allies.

This strategy demonstrates how hybrid warfare enables gradual, almost imperceptible

shifts in the balance of power. By staying below the threshold of conventional war, China has expanded its control without provoking a direct confrontation with stronger military alliances.

Implications for Security and Sovereignty

Hybrid warfare represents a profound challenge to traditional notions of national security and sovereignty. Unlike conventional conflicts where borders, armies, and battlefields are clearly defined, hybrid warfare operates in a gray zone—a space where the lines between war and peace, civilian and military, are deliberately blurred. This creates unique vulnerabilities for nation-states, forcing them to rethink not only military strategy but also governance, law, and societal resilience.

1. Sovereignty Under Strain

Hybrid warfare undermines the traditional concept of state sovereignty. When adversaries employ covert operations, proxy forces, or cyberattacks, the state may struggle to identify the aggressor and respond in a timely manner. This ambiguity weakens a nation's ability to defend its borders and maintain control over its own affairs. The gradual, incremental nature of hybrid tactics—economic pressure, disinformation campaigns, or strategic infiltration—can erode a state's autonomy without triggering formal war, leaving policymakers in a constant state of uncertainty.

2. Civilian Infrastructure and Societal Vulnerability

In hybrid conflicts, civilian infrastructure becomes a primary target. Power grids, communication networks, financial institutions, and social media platforms are all susceptible to attacks, making the public both the audience and the battlefield. Disruption in these areas can paralyze governance, reduce public trust, and create social unrest. Unlike conventional war, where military assets are directly attacked, hybrid strategies deliberately focus on the civilian sphere, creating long-lasting and widespread societal impact.

3. Challenges to Democratic Institutions

Modern hybrid warfare often includes disinformation campaigns designed to influence public opinion, disrupt elections, and polarize societies. Democracies, which rely on transparency, freedom of expression, and public trust, are particularly vulnerable. When false narratives spread rapidly through social media and online platforms, they can weaken

the legitimacy of institutions and create internal instability, effectively achieving strategic objectives without any overt military action.

4. Legal and Normative Gaps

The international legal framework is not yet fully equipped to address hybrid tactics. Actions such as cyberattacks, economic coercion, and proxy warfare often fall into legal gray areas, making accountability and retaliation difficult. Traditional laws of war are designed for conventional battles and struggle to adapt to scenarios where aggression is covert, deniable, and multi-dimensional. This creates a challenge for global governance and cooperative security mechanisms, leaving states exposed to persistent, low-intensity threats.

5. Strategic Uncertainty and Defense Dilemmas

Hybrid warfare complicates strategic planning for national defense. Military responses alone are insufficient because threats extend into cyberspace, media, and economic domains. States must prepare for multiple contingencies simultaneously, balancing the need for deterrence with the risk of over-militarizing society. Strategic uncertainty also challenges alliances; collective defense mechanisms like NATO's Article 5 rely on clear attribution, which hybrid tactics deliberately obscure.

6. The Need for a Holistic Security Approach

Given these multifaceted challenges, hybrid warfare demands a holistic, integrated approach to security. Nations must develop resilience across political, economic, social, and technological domains. This includes strengthening critical infrastructure, enhancing cybersecurity, improving intelligence capabilities, and fostering public awareness to counter disinformation. Hybrid threats underscore that sovereignty is not just about territorial integrity but also about the state's capacity to maintain functional institutions, social cohesion, and strategic autonomy in a complex, interconnected world.

Policy Responses to Hybrid Warfare

The complex and multi-dimensional nature of hybrid warfare requires nations to move beyond conventional military thinking. Traditional defense mechanisms are insufficient when threats extend into cyberspace, economic domains, media, and social infrastructure. To effectively respond, states must adopt a comprehensive, multi-layered strategy that integrates military readiness, governance, technological safeguards, and societal resilience.

1. Integrated National Security Strategy

Hybrid threats demand that defense planning be coordinated across all arms of government. Security cannot be the sole responsibility of the military; intelligence agencies, law enforcement, diplomatic corps, and economic regulators must operate in synergy. This integrated approach ensures that threats—from cyberattacks to proxy insurgencies—are identified early, assessed holistically, and countered efficiently. By breaking down silos between agencies, states can respond faster and with greater precision, reducing vulnerabilities in both overt and covert domains.

2. Cybersecurity and Technological Resilience

Cyber operations are a core component of hybrid warfare, targeting critical infrastructure, financial systems, and information networks. Nations must invest in robust cybersecurity architecture, including regular audits, intrusion detection systems, and rapid response teams. Training government personnel, private sector stakeholders, and citizens to recognize and respond to cyber threats is equally vital. Developing indigenous technological capabilities ensures that states are not overly dependent on foreign expertise, reducing strategic vulnerabilities.

3. Countering Disinformation and Strategic Communication

Disinformation campaigns erode trust in institutions, polarize societies, and manipulate public opinion. Effective countermeasures involve proactive communication strategies that are transparent, credible, and culturally sensitive. Governments should work with media organizations, fact-checking agencies, and civil society to identify false narratives and provide verified information quickly. Education initiatives that enhance media literacy among citizens also help create a resilient society capable of resisting manipulative campaigns.

4. Strengthening Critical Infrastructure and Civil Preparedness

Hybrid warfare often targets civilian systems—energy grids, transportation networks, water supplies, and communication channels. States must prioritize the resilience of these infrastructures, ensuring redundancy, secure backup systems, and rapid restoration protocols. Civil preparedness programs, such as emergency drills and public awareness campaigns, help communities adapt to crises and maintain confidence in state institutions.

A society that can endure disruptions without descending into chaos is a strategic asset in hybrid conflict.

5. Legal and Policy Frameworks

Many hybrid tactics operate in legal gray zones, making accountability challenging. Nations should update laws to address cybercrimes, disinformation campaigns, and irregular warfare tactics. Establishing clear rules for state and non-state actors, including consequences for violations, strengthens deterrence. International cooperation is also essential: sharing intelligence, developing norms for cyberspace, and establishing treaties to address cross-border hybrid threats can reduce ambiguity and hold perpetrators accountable.

6. Regional and Global Cooperation

Hybrid threats rarely respect national boundaries. Regional alliances and international partnerships are crucial for early warning, intelligence sharing, and coordinated response. Collaborative exercises, joint cybersecurity initiatives, and diplomatic coordination enhance collective resilience. By pooling resources and expertise, nations can create deterrents that extend beyond individual borders and ensure that hybrid aggression faces a coordinated, multilateral response.

7. Human and Societal Resilience

Finally, the human dimension is central to countering hybrid warfare. Public trust, social cohesion, and citizen awareness are as important as military strength. Policies should foster civic engagement, strengthen democratic institutions, and encourage societal resilience. A well-informed and united population is less susceptible to manipulation, reducing the effectiveness of hybrid tactics aimed at sowing discord.

Critiques of the Hybrid Warfare Concept

Despite its widespread use in contemporary security studies, the concept of hybrid warfare has faced significant criticism from scholars and military analysts. One of the main concerns is conceptual ambiguity. Hybrid warfare is often defined so broadly that it encompasses everything from cyberattacks and disinformation campaigns to proxy wars and economic coercion. This expansive definition can make it difficult to distinguish

hybrid warfare from traditional asymmetric or irregular conflicts, potentially reducing the concept's analytical precision and utility in guiding policy. Critics also point out that hybrid tactics are not entirely novel. Many of the strategies associated with hybrid warfare; such as propaganda, covert operations, alliances with non-state actors, and economic manipulation have been employed throughout history, from medieval political maneuvers to Cold War proxy conflicts. What distinguishes modern hybrid warfare is less the methods themselves and more their integration across multiple domains, aided by technological advancement.

Another significant concern is the potential for over-militarization. Because hybrid threats operate in ambiguous gray zones, states may feel compelled to expand surveillance, enhance domestic security measures, or militarize civilian spaces to preempt attacks. While intended to protect national security, such measures can inadvertently weaken civil liberties and erode public trust, undermining societal resilience; the very attribute essential for countering hybrid threats. Closely linked to this is the problem of attribution and accountability. Hybrid operations are deliberately deniable, making it difficult to establish clear responsibility, especially in cyberattacks or disinformation campaigns. This ambiguity can hinder deterrence and create opportunities for adversaries to act with impunity, complicating both national and international responses.

Critics further argue that the concept of hybrid warfare can encourage strategic misinterpretation or policy overreach. Governments might perceive threats in routine political competition, social movements, or economic pressure, mistakenly classifying them as hostile hybrid operations. Such misinterpretations can lead to misallocation of resources, unnecessary tensions, and even domestic or international overreaction. Finally, hybrid warfare presents significant challenges for measurement and evaluation. Its combination of overt and covert actions across military, cyber, economic, and informational domains makes it difficult to empirically assess its effectiveness or prevalence. Without reliable metrics, it becomes challenging for policymakers to determine which strategies are genuinely effective, limiting the concept's practical application in shaping defense or security planning.

In sum, while hybrid warfare provides a valuable lens for understanding the evolving nature of modern conflict, these critiques highlight the need for conceptual clarity, careful operational definitions, and balanced policy responses. Recognizing the limitations of the

concept ensures that states can respond effectively to contemporary threats without overreacting or compromising democratic values and societal cohesion.

Conclusion

In conclusion, security today can no longer be explained only through the familiar categories of conventional or asymmetric warfare. The rise of hybrid warfare has blurred those boundaries, combining traditional military force with cyberattacks, propaganda, economic disruption, and the involvement of non-state players. Conflicts are no longer fought just on battlefields; they unfold in digital spaces, in financial markets, and within the minds and perceptions of ordinary people. This change has widened the scope of what it means to protect a nation and its sovereignty.

Security in this new era is less about stockpiling weapons and more about building resilience. It depends on how effectively societies can absorb shocks, respond to crises, and rebuild after disruption. Strong institutions, credible leadership, and public trust become as important as defense systems. Without the confidence of its people, even the most powerful state becomes vulnerable. Hybrid threats also show that no country can stand alone. Because cyber networks, trade systems, and narratives cross borders, cooperation among nations is essential to defend against such fluid and unpredictable dangers.

Rethinking security through the lens of hybrid warfare reminds us that strength today is measured not only by deterrence but also by adaptability, inclusiveness, and foresight. It is about protecting the integrity of societies, preserving human dignity, and ensuring that communities remain united in the face of manipulation and uncertainty. Ultimately, true security lies in the capacity of states and citizens to confront challenges together and safeguard the values that hold them together.

References

- Chivvis, C. S. (2017). *Understanding Russian “hybrid warfare” and what can be done about it*. RAND Corporation.
- Giles, K. (2016). *Russia’s ‘new’ tools for confronting the West: Continuity and innovation in Moscow’s exercise of power*. Chatham House.
- Hoffman, F. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies.
- Kaldor, M. (2012). *New and old wars: Organized violence in a global era* (3rd ed.). Stanford University Press.
- NATO. (2020). *NATO’s approach to countering hybrid threats*. Brussels: NATO Public Diplomacy Division.

- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media*. Houghton Mifflin Harcourt.
- Murray, Williamson, and Peter R. Mansoor, eds. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge University Press, 2012.
- Frank G. Hoffman, "Future Threats and Strategic Thinking," *Infinity Journal*, Issue 4 (Fall 2011).
- Charap, Samuel. "The Ghost of Hybrid War." *Survival* 57, no. 6 (2015): 51-58.
- Casey-Maslen, Stuart. *Hybrid Warfare under International Law*. Hart Publishing, 2024.
- Ofer Fridman

CITATION:

Ruby, D. (2025). Beyond Conventional and Asymmetric War: Rethinking Security through Hybrid Warfare. In INNOVATIVE RESEARCH THOUGHTS IN SOCIAL SCIENCES (Vol. 1, Number 2, pp. 61–72). Zenodo.