

Hybrid Warfare and National Security: India's Strategic Response to Cyber Threats, Information Warfare, and Transnational Terrorism

Dr. Ravindra S. Marathe*

Assistant Professor & Head, Department of Defence & Strategic Studies, Pratap College (Autonomous), Amalner, Dist- Jalgaon, Maharashtra.

*Corresponding Author: rsmarathe9@gmail.com

Abstract

Hybrid warfare has emerged as one of the most significant challenges to national security in the contemporary international system. It combines conventional military capabilities with non dynamic tools such as cyber operations, information warfare, proxy terrorism, economic pressure, and political influence activities. India witnesses persistent hybrid threats arising from its complex regional environment, unresolved territorial disputes, rapid digital transformation, and open democratic society. Cyber intrusions targeting critical infrastructure, coordinated disinformation campaigns across digital platforms, and cross border terrorism supported by external actors illustrate the evolving character of conflict confronting the Indian state. This paper examines hybrid warfare as a strategic framework and analyses its key dimensions relevant to India's national security, namely cyber threats, information warfare, and transnational terrorism. It critically evaluates India's existing institutional, legal, and policy responses and identifies structural and strategic gaps. The paper argues that India requires an integrated and proactive national approach that combines cyber resilience, counter terrorism, strategic communication, and diplomacy. Strengthening these capabilities is essential for safeguarding India's security interests and for supporting its broader foreign policy objectives in a rapidly evolving multi-polar world.

Keywords: Hybrid Warfare, National Security, Cyber Security, Information Warfare, Terrorism, India.

Introduction

The character of warfare and conflict in international relations has undergone a profound transformation in the twenty first century. Traditional distinctions between war and peace have become increasingly blurred. States today face persistent security challenges that operate below the threshold of declared war yet generate significant strategic consequences. These challenges exploit political, technological, social, and economic vulnerabilities rather than relying solely on conventional military force. This evolving security environment has given rise to the concept of hybrid warfare. Hybrid warfare represents a mode of conflict in which state and non state actors employ a coordinated mix of military and non military instruments to achieve political objectives. These instruments include cyber attacks, disinformation campaigns, proxy violence, economic coercion, diplomatic pressure, and psychological operations. The objective is to weaken the adversary internally, create strategic confusion, and constrain effective response, while avoiding escalation into open war.

For India, hybrid warfare poses a particularly serious challenge. India's security environment is shaped by unresolved border disputes, long standing cross border terrorism, strategic rivalry with major powers, and increasing integration into the global digital economy. At the same time, India's democratic system, social diversity, and open information space create vulnerabilities that adversaries can exploit. Hybrid strategies allow hostile actors to target India's internal cohesion, economic stability, and

*Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.

*A Special Issue for the papers accepted for publication in the International Multidisciplinary Conference on India's Foreign Policy and International Relations: A Future Roadmap (IFPIR-2026) (Hybrid Mode)(22-24 January 2026) Organized by Geo-Politics & Defence Study Research Cell, Faculty of Arts, Education and Social Sciences, Jai Narain Vyas University, Jodhpur, Rajasthan.

international image without triggering direct military retaliation. Recent developments illustrate this challenge clearly. Cyber attacks on critical infrastructure, coordinated misinformation during political and security crises, and terrorist violence supported through transnational networks are no longer isolated incidents. They form part of a broader pattern of indirect conflict. Understanding how these elements interact is essential for assessing India's national security preparedness and shaping its future strategic choices.

This paper examines hybrid warfare in the Indian context by focusing on three interlinked dimensions. Cyber threats, information warfare, and transnational terrorism. It evaluates India's current policy responses and institutional arrangements and proposes measures to enhance national resilience. The analysis is situated within the broader framework of international relations and security studies, emphasizing the implications for India's regional and global role.

Objectives of the Paper

- To examine the nature and core components of hybrid warfare in the contemporary security environment.
- To analyze the impact of hybrid warfare on India's national security framework.
- To evaluate India's strategic and institutional responses to hybrid warfare.

Hypotheses

- Hybrid Warfare poses a grater long term threats to India's national security than conventional military conflict.
- India's current national security responses are fragmented when dealing with multi domain hybrid threats.

Research Methodology

This study follows a qualitative and analytical research methodology. The paper uses a descriptive approach to explain the concept of hybrid warfare and an analytical approach to assess its implications for India's national security.

Hybrid Warfare as a Strategic Concept

Hybrid warfare is best understood as a strategy rather than a single method of conflict. It involves the deliberate integration of multiple tools of state power to achieve political objectives. These tools are employed simultaneously and adaptively, exploiting the adversary's weaknesses across different domains. A defining characteristic of hybrid warfare is ambiguity. Actions are designed to obscure responsibility and intent. Cyber attacks can be routed through multiple jurisdictions. Disinformation can be disseminated through seemingly independent actors. Proxy groups can be portrayed as domestic movements rather than instruments of foreign policy. This ambiguity complicates attribution and delays response, thereby increasing the effectiveness of hybrid strategies.

Another central feature is the expansion of the battlefield. Hybrid warfare shifts conflict from traditional military arenas to civilian domains. Financial systems, energy grids, communication networks, educational institutions, and media platforms become targets. The aim is not immediate territorial gain but long term strategic erosion. By undermining public trust in institutions and weakening governance capacity, hybrid warfare seeks to achieve outcomes that conventional military force alone cannot deliver. Hybrid warfare also exploits legal and normative gaps. International law remains largely focused on armed conflict between states. Hybrid actions often fall below established thresholds of armed attack, allowing adversaries to operate in gray zones with limited accountability. This creates strategic dilemmas for states committed to legal and normative restraint.

For India, this strategic environment demands a reassessment of traditional security thinking. Military deterrence remains necessary but insufficient. Effective response to hybrid warfare requires coordination across military, diplomatic, economic, technological, and informational domains.

Cyber Threats and India's National Security

Cyber space has emerged as one of the most critical arenas of hybrid conflict. India's rapid digital transformation has brought significant economic and social benefits. Digital governance initiatives, online financial systems, and expanding internet access have improved efficiency and inclusion. However, this transformation has also created new vulnerabilities. India's critical infrastructure increasingly relies on networked digital systems. Power generation and distribution, transportation

networks, banking and financial services, healthcare systems, and defence communication platforms depend on cyber enabled technologies. Disruption of these systems can have immediate and far reaching consequences for national security and public confidence. India has experienced a steady increase in cyber incidents. These include data breaches affecting government and private databases, ransomware attacks on hospitals and enterprises, and attempted intrusions into strategic networks. Many of these activities are attributed to advanced persistent threat groups linked to foreign states, particularly during periods of political or military tension. This pattern suggests that cyber operations are being used as strategic tools rather than isolated criminal acts. In the context of hybrid warfare, cyber operations serve multiple functions. They facilitate espionage by extracting sensitive information. They disrupt essential services, creating economic and social stress. They signal capability and resolve without crossing conventional red lines. They also generate uncertainty by demonstrating the state's vulnerability to unseen threats.

India has taken important steps to address cyber security challenges. Institutional mechanisms such as the Indian Computer Emergency Response Team, sector specific cyber security guidelines, and the recognition of cyberspace as a military domain reflect growing awareness. However, these efforts face structural limitations. Coordination between civilian agencies, military organizations, and state governments remains uneven. Cyber security expertise is concentrated in limited pockets, while demand far exceeds supply. Dependence on imported hardware and software exposes India to supply chain risks. Moreover, the private sector controls much of the digital infrastructure, complicating regulatory oversight and response coordination. Without addressing these challenges, India's cyber defences will remain reactive rather than resilient. In a hybrid warfare environment, resilience is as important as deterrence.

Information Warfare and Strategic Communication

Information warfare constitutes another core pillar of hybrid conflict. It seeks to influence perceptions, attitudes, and behavior rather than physical assets. Control over narratives has become a decisive factor in shaping political outcomes and security dynamics. India's open media environment and social diversity create both strengths and vulnerabilities. A free press and active civil society enhance democratic accountability. At the same time, these features provide fertile ground for disinformation campaigns. Social media platforms allow false narratives to spread rapidly and widely, often outpacing official clarification.

Information warfare in the Indian context operates at multiple levels. Domestically, it seeks to exploit social divisions, inflame communal tensions, and undermine trust in democratic institutions. During elections, protests, or security crises, coordinated misinformation can distort public debate and weaken state authority. Internationally, information warfare targets India's image and diplomatic standing. Narratives portraying India as unstable, intolerant, or unreliable can influence foreign public opinion and policy decisions. This has implications for trade, investment, and strategic partnerships. India has responded with measures such as fact checking initiatives, platform level content moderation, and public awareness campaigns. While necessary, these measures face inherent limitations. Technological innovation often outpaces regulation. Excessive control risks undermining free expression and democratic legitimacy.

A major weakness lies in the absence of a unified strategic communication framework. Government messaging is often fragmented across agencies and levels of administration. Responses tend to be reactive rather than anticipatory. In hybrid warfare, credibility, consistency, and speed are essential. Without a coherent narrative strategy, counter disinformation efforts struggle to gain public trust.

Transnational Terrorism within Hybrid Warfare

Terrorism remains one of the most persistent and emotionally charged security challenges confronting India. In the context of hybrid warfare, terrorism functions as a proxy instrument that complements cyber and information operations. Cross border terrorism in regions such as Jammu and Kashmir illustrates how terrorist violence is integrated into broader hybrid strategies. Attacks generate fear and instability, while accompanying propaganda seeks to frame violence as indigenous resistance. This dual approach complicates India's response by combining physical harm with narrative manipulation. Terrorist organizations have adapted to technological change. Encrypted communication platforms, online recruitment tools, and digital financial channels enable transnational coordination with minimal physical presence. Cyber space reduces operational costs and increases reach, making counter terrorism more complex.

India has strengthened its counter terrorism capabilities over time. Intelligence sharing among agencies has improved. Legal instruments allow the disruption of financing networks and the designation of terrorist organizations. Military responses and diplomatic engagement signal resolve and deterrence. However, terrorism within a hybrid warfare framework cannot be defeated through force alone. Ideological narratives, online radicalization, and external sponsorship networks require political, informational, and diplomatic engagement. Failure to address these dimensions allows terrorist ecosystems to regenerate despite tactical successes.

Regional Security Implications of Hybrid Warfare

Hybrid warfare has significant implications for regional security and stability. South Asia is characterized by strategic mistrust, unresolved disputes, and limited institutional cooperation. Hybrid tactics further erode confidence and complicate crisis management. India's relations with Pakistan and China illustrate how hybrid methods operate alongside conventional deterrence. Cyber intrusions, influence operations, and proxy activities occur in parallel with military posturing and diplomatic engagement. This layered approach increases strategic uncertainty and the risk of miscalculation. Smaller states in the region also become arenas of hybrid competition. Political influence operations, economic leverage, and information campaigns affect regional alignments and governance outcomes. For India, this environment challenges traditional approaches to regional leadership.

Hybrid warfare lowers the threshold of conflict by normalizing hostile actions below the level of war. This creates a persistent state of competition rather than episodic crises. Managing this environment requires sustained engagement rather than reactive responses. India's ability to promote regional stability depends on enhancing collective resilience. Cyber cooperation, intelligence sharing, and capacity building with neighboring states can reduce vulnerabilities. Ignoring the regional dimension of hybrid warfare weakens India's strategic position.

Some Case Studies

Pegasus controversy and political surveillance, 2019 to 2021

The Pegasus Project investigation in 2021 exposed the risks posed by commercial spyware. Journalists and civil society organizations revealed alleged targeting of journalists, politicians, and activists. The case highlighted three policy points for India.

- Dual use of cyber tools: Commercial surveillance software may be used for national security. It may also be used for political ends. Oversight and legal clarity are required.
- Domestic political effect: Allegations of unlawful surveillance erode public trust and weaken institutional legitimacy. That creates strategic vulnerability in hybrid competition.
- International norms: Use of spyware by or against state actors has transnational consequences. It shapes alliances and constrains diplomatic leverage.

The Pegasus case is not an attack on infrastructure. It is an example of information and surveillance risks inside hybrid conflict. It proves that militant tradecraft has become widely available. Policy must reflect that reality.

Pulwama attack and Balakot strike, 2019

The February 2019 Pulwama attack and India's February 2019 Balakot response illustrate how terrorism, political messages, and military action can cohere into a hybrid episode. The Pulwama suicide bombing produced a strong domestic reaction. India responded with the air strike in Balakot. The episode shows two dynamics.

- Proxy and plausible deniability: Terror groups with cross border reach can be used as instruments of pressure while offering deniability to sponsoring states. The 2019 crisis demonstrated how violent acts feed political narratives at home and abroad.
- Rapid narrative contest: Within hours, competing narratives sought to shape international opinion. Both state and non state actors used traditional and social media to influence outcomes.

India's response combined kinetic action, diplomatic engagement, and public messaging. The episode underlines the need to plan integrated responses that combine law enforcement, military deterrence, and strategic communication.

Galwan Valley Clash, 2020, and Associated Cyber and Information Activity

The 2020 Galwan valley clash with Chinese forces included kinetic confrontation on the ground. It also triggered waves of cyber probes and information activity directed at India. Analysts reported a surge of cyber attacks and a coordinated online campaign to shape perceptions during and after the clash. Sources record large numbers of cyber probes against Indian networks in the period following the clash. These probes aimed to gather intelligence and to shape the information environment.

The Galwan episode shows how conventional border confrontation and hybrid activity combine. It also illustrates the strategic logic of escalation below the threshold of full war.

SideCopy and other APT campaigns targeting Indian defence networks, 2023

Security reporting in 2023 documented the SideCopy campaign. The campaign targeted Indian defence related networks and government assets. Analysts linked the campaign to advanced persistent threat actors operating from Pakistan origin infrastructure. The campaign used data exfiltration and covert backdoors. Reporting indicates that government ministries and defence research organizations were among targets.

The SideCopy and similar campaigns reveal persistent espionage threats. They show that state and non state actors use tailored cyber tools to access sensitive information. That undermines strategic secrecy and affects force readiness.

Ransomware and Attacks on Healthcare and Defence Related Facilities

Ransomware attacks hit Indian hospitals and firms in 2021 and 2022. Health sector incidents expose life critical vulnerabilities. In 2023 a ransomware attack affected a defence unit. Ransomware is both criminal profit seeking activity and a coercive tool within hybrid operations. An attack on health infrastructure during a national emergency would create political pressure. Recent incidents show the need for sector specific resilience plans.

Evaluation of India's Strategic Response

India has increasingly acknowledged the changing character of conflict. Policy documents and military doctrines reflect growing awareness of nontraditional threats. Institutional developments in cyber and space domains demonstrate adaptation. Despite these advances, India's response to hybrid warfare remains fragmented. Institutional silos persist between civilian and military agencies. Legal frameworks struggle to keep pace with technological change. Research and innovation ecosystems require stronger support.

Strategic culture also shapes outcomes. India has traditionally emphasized restraint and reactive responses. Hybrid warfare demands anticipation, resilience, and proactive narrative control. Without these, deterrence remains incomplete. Human capital constraints further limit effectiveness. Cyber security, data analysis, and strategic communication require specialized skills that are in short supply. Education and training systems must align more closely with security needs.

Policy Recommendations

India requires a comprehensive and integrated approach to counter hybrid warfare.

- Establish centralized coordination mechanisms that integrate cyber security, information management, intelligence, and military planning under clear political oversight.
- Invest in cyber resilience through indigenous technology development, public private partnerships, and nationwide cyber hygiene programs.
- Develop a coherent strategic communication doctrine focused on credibility, transparency, and rapid response, supported by institutional capacity.
- Address terrorism through a hybrid framework that combines force, financial disruption, cyber monitoring, ideological counter narratives, and sustained diplomacy.
- Strengthen regional and international cooperation to share intelligence, develop norms, and build collective resilience against hybrid threats.
- Align foreign policy instruments with hybrid security objectives while preserving strategic autonomy and democratic values.

Conclusion

Hybrid warfare represents a fundamental shift in the nature of conflict in international relations. For India, cyber threats, information warfare, and transnational terrorism form an interconnected security challenge that cannot be addressed through conventional military means alone.

India has made important strides in recognizing these threats. However, gaps in coordination, capability, and strategic vision remain. Addressing these gaps is essential for protecting national security, maintaining internal stability, and supporting India's aspirations as a responsible global actor.

Strengthening resilience against hybrid warfare will enhance India's strategic autonomy, improve regional stability, and reinforce its role in a rapidly evolving multipolar world.

References

1. Ahuja, Amit and Kapur, Devesh (eds.). Internal Security in India: Violence, Order, and the State, Oxford University Press, New York, 2023.
2. Deshpande, Vikrant, Hybrid Warfare: The Changing Character of Conflict, Institute for Defence Studies & Analyses, Pentagon Press, New Delhi, 2018.
3. Pandit, Rahul, Information Warfare: Battleground of the Digital Age, Nation Press, Chennai, 2025.
4. Clarke, Richard A. and Knake, Robert K., Cyber War: The Next Threat to National Security and What to Do About It. Ecco, New York, 2012.
5. Hoffman, Frank G., Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington, Virginia. 2007.
6. Ministry of Defence. Government of India. Annual Report. 2023-24.
7. Tellis, A. 2017. India's Emerging Strategic Challenges. Carnegie Endowment for International Peace.
8. United Nations Office of Counter-Terrorism, UNGlobal Counter-Terrorism Strategy Review. United Nations, New York. 2023
9. Ministry of Electronics and Information Technology. CERT-In annual reports 2021, 2022, 2023. [Indian - Computer Emergency Response Teamwww.cert-in.org.in](http://www.cert-in.org.in)
10. Pegasus Project. 2021. Investigative reports by consortium of media organizations and Amnesty International. <https://www.scoobserver.in/cases/manohar-lal-sharma-v-union-of-india-pegasus-spyware-probe-case-background/>
11. Ministry of External Affairs. 2019. Statement on Balakot strike and related exchanges. Government of India. <https://www.mea.gov.in/media-briefings.htm?dtl%2F31090%2FStatement+by+Foreign+Secretary+on+26+February+2019+on+the+Strike+on+JeM+training+camp+at+Balakot=&>
12. CENJOWS analysis. 2025. China's informatized warfare and disinformation during and after the Galwan valley clash. Centre for Joint Warfare Studies. <https://cenjows.in/publications/chinas-informatized-warfare-and-disinformation-during-and-after-the-galwan-valley-clash>
13. The Hacker News. 2023. SideCopy linked to cyberattacks on Indian defence networks. <https://thehackernews.com/2023/03/pakistan-origin-sidecopy-linked-to-new.html>
14. VIF Cyber Review. 2022. Voluntary reports on Indian cyber incidents and sector vulnerabilities. <https://www.vifindia.org/print/11100?via=Azure&>
15. Vajiram and Ravi. 2024. Report on 2023 ransomware incident affecting Indian defence units. <https://vajiramandravi.com/current-affairs/2023-ransomware-attack-on-indian-defence-unit-a-dopt-report-insight/>.

