

Hybrid Warfare, Meaning, Dimensions, Examples, Challenges

July 22, 2026 • vajiramandravi.com



Hybrid warfare is a modern form of conflict that combines conventional military force with cyberattacks, disinformation, proxy warfare, economic pressure and other covert methods. It creates security challenges that go beyond the traditional battlefield, making hybrid warfare an important concern for India's national security and preparedness.

Hybrid Warfare Meaning

Hybrid warfare refers to the **coordinated use of military and non-military, overt and covert means to achieve strategic objectives**. It may combine conventional forces with **cyberattacks, disinformation, economic pressure, irregular armed groups** and **other non-conventional methods**. Its **objective** is often to blur the line between war and peace, exploit vulnerabilities and weaken the target without necessarily engaging in a conventional war.

Hybrid Warfare Dimensions

Hybrid warfare operates across multiple domains and derives its strength from the combination of different tools:

- **Military and proxy warfare:** Use of regular forces, terrorist groups, militias and other irregular actors to achieve strategic objectives.
- **Cyber warfare:** Targeting government networks, defence systems, financial institutions and critical infrastructure to disrupt essential services.
- **Information and cognitive warfare:** Use of disinformation, propaganda and manipulated content to influence public opinion, create confusion and weaken trust in institutions.
- **Economic coercion:** Use of trade restrictions, financial pressure, technological dependence and disruption of strategic supply chains.
- **Drone and emerging technology warfare:** Use of drones, artificial intelligence and other technologies for surveillance, infiltration and attacks.
- **Sabotage and espionage:** Covert efforts to damage infrastructure, obtain sensitive information or disrupt state functioning.
- **Political and societal influence:** Exploitation of social divisions and institutional vulnerabilities to undermine internal stability.

Hybrid Warfare Examples

Recent conflicts show that hybrid warfare combines military force with cyber, economic, information and covert methods:

- **US-Israel-Iran Conflict (2026):** Missile and drone strikes were combined with attacks on shipping, ports, energy infrastructure and strategic trade routes, showing how economic chokepoints can become instruments of warfare.
- **Russia-Ukraine War and Baltic Region:** Conventional warfare has been accompanied by cyberattacks, disinformation, electronic warfare, drone strikes and alleged threats to undersea cables and critical infrastructure, often creating ambiguity about responsibility.
- **China-Taiwan:** China combines military pressure, drone and balloon activities, disinformation and psychological operations to influence Taiwan while remaining below the threshold of open war.
- **Operation Sindoor (2025):** India's precision strikes against terrorist infrastructure were accompanied by drone and missile operations, cyber threats and information warfare, reflecting the increasingly multi-domain nature of conflict.

These examples show that hybrid warfare exploits different vulnerabilities – economic routes, critical infrastructure, technology, public opinion and security networks through a combination of overt and covert methods.

Challenges in Countering Hybrid Warfare

Hybrid warfare is difficult to counter because its methods are diverse, ambiguous and constantly evolving:

- **Attribution challenge:** Covert operations, proxies and cyber tools make it difficult to identify the real attacker.

- **Blurred response threshold:** It may be difficult to determine whether an incident requires a military, diplomatic, cyber or law-enforcement response.
- **Institutional silos:** Hybrid threats cut across the responsibilities of defence, intelligence, home affairs, state police and private organisations.
- **Speed of disinformation:** False narratives can spread rapidly, often faster than official verification and response.
- **Critical infrastructure vulnerability:** Increasing digital dependence exposes power, telecom, financial and other essential systems to disruption.
- **Technological dependence:** Dependence on foreign technologies and strategic supply chains can create security vulnerabilities.
- **Civil liberties concerns:** Countering disinformation and hostile influence must be balanced with democratic freedoms and legitimate public debate.

Hybrid Warfare and India's Preparedness

India is strengthening its preparedness against hybrid warfare through multi-domain integration, cyber resilience, technological self-reliance and a whole-of-nation approach. Recent government initiatives and defence reforms include:

- **Multi-domain operations:** India has released the Joint Doctrine for Multi-Domain Operations, integrating the land, sea, air, space, cyber and cognitive domains for joint military operations.
- **Cyber preparedness:** The Joint Doctrine for Cyberspace Operations provides a unified framework for integrating offensive and defensive cyber capabilities, real-time intelligence and cyber resilience across the three Services.
- **Protection of critical infrastructure:** **CERT-In** responds to cybersecurity incidents, while **NCIIPC** is the national nodal agency for protecting Critical Information Infrastructure.
- **Future warfare preparedness:** The Tri-Services Future Warfare Course brings together the Armed Forces, DRDO, academia, startups and industry to build capabilities in AI, autonomous systems, unmanned platforms and cybersecurity.
- **Jointness and interoperability:** Initiatives such as **Ran Samwad** and **All Domain Joint Operations exercises** focus on integrated planning, intelligence sharing, interoperable command and control, and coordinated responses across domains.
- **Whole-of-nation approach:** The government increasingly recognises that national security requires cooperation among the Armed Forces, government agencies, technology institutions, industry, academia and society.

Thus, India is moving from a traditional domain-based security approach towards integrated, multi-domain and resilient preparedness to counter hybrid threats.

Way Forward

India needs to build resilience across institutions, infrastructure, technology and society to effectively counter hybrid warfare:

- **Strengthen whole-of-government coordination:** Improve real-time information sharing among defence, intelligence, cyber, diplomatic and law-enforcement agencies.
- **Build critical infrastructure resilience:** Strengthen cyber audits, continuous monitoring, redundancy and rapid incident-response mechanisms.
- **Develop strategic communication:** Ensure timely, credible and fact-based communication during security crises.
- **Strengthen intelligence and early warning:** Use AI, data analytics, satellite systems and real-time intelligence to detect coordinated threats.
- **Secure strategic supply chains:** Reduce dependence on external sources for critical technologies, energy, telecommunications and strategic materials.
- **Promote public-private cooperation:** Integrate technology companies, startups, academia and the private sector into national security preparedness.
- **Deepen multi-domain jointness:** Integrate capabilities across land, sea, air, space, cyber and cognitive domains.
- **Improve public awareness:** Build media and digital literacy to reduce the impact of disinformation and manipulation.

Hybrid warfare requires a response that is as integrated as the threat itself. India's preparedness must therefore combine military capability with cyber resilience, technological self-reliance, institutional coordination, strategic communication and societal awareness.

Source: <https://vajiramandravi.com/current-affairs/hybrid-warfare/>

© Vajiram & Ravi. For personal use only.