

**NEXT IAS**

# **DAILY EDITORIAL ANALYSIS**

TOPIC

---

**MODERN, ASYMMETRIC & HYBRID  
WARFARE**

---

[www.nextias.com](http://www.nextias.com)

## MODERN, ASYMMETRIC & HYBRID WARFARE

### Context

- A recent asymmetric strike by Ukraine under the **Operation Spiderweb**, which involved long-range drone assaults on Russian air bases has drawn significant attention, offering **key lessons in modern warfare**.

### Ukraine's Asymmetric Strike

- **Strategic Targeting:** Ukraine's drone strikes damaged or destroyed over 40 Russian warplanes, including those stationed in remote regions.
  - ♦ It highlights the effectiveness of precision attacks on high-value assets.
- **Psychological Impact:** The strike not only inflicted material losses but also undermined Russian air superiority, forcing adjustments in deployment strategies.
- **Lessons for Future Conflicts:** The attack underscores the growing role of unmanned aerial systems (UAS) in modern warfare, emphasizing the need for robust air defense mechanisms.

### Understanding Modern, Hybrid, and Asymmetric Warfare

- Modern warfare integrates advanced technology, cyber capabilities, and artificial intelligence to enhance military operations.
- Nations are increasingly **relying on drones, hypersonic missiles, and electronic warfare** to disrupt enemy defenses.
- **Hybrid Warfare** is **non-linear and unpredictable**, and designed to destabilize adversaries without direct military confrontation.
  - ♦ It involves a **mix of kinetic** (*traditional military operations*) and **non-kinetic** (*extends beyond usual military operations*) tactics, including cyber warfare, disinformation campaigns, economic coercion, and proxy conflicts etc.
- **Asymmetric warfare** occurs when a weaker force uses **unconventional tactics** to counter a stronger adversary. It includes *guerrilla warfare, cyberattacks, and drone strikes*.
  - ♦ The **Russia-Ukraine conflict** is a prime example, where cyberattacks, drone warfare, and economic sanctions have played a crucial role.

### Key Reasons for Their Emergence and Increased Prominence

- **Strategic Advantage and Deniability:** Hybrid and asymmetric approaches allow actors to achieve political, military, or economic objectives without a formal declaration of war. This keeps avenues for diplomatic negotiations open and minimizes the risk of direct, high-intensity confrontation.
- **Cost-Effectiveness:** These methods are generally less costly and logistically less complex than deploying large conventional military forces. Economic sanctions, cyberattacks, and supporting proxy groups can inflict significant damage on an adversary's economy or infrastructure without the heavy investment in military personnel and hardware.
- **Technological Advancements:** Relatively low-cost, high-tech weapons (e.g., drones, precision-guided missiles) are increasingly available to non-state actors, leveling the playing field against technologically superior conventional forces.
- **Rise of Non-State Actors and Proxy Warfare:** The post-Cold War era has seen a proliferation of powerful non-state actors (terrorist groups, insurgencies, private military companies) that can operate across borders and engage in complex networks of alliances.
- **Information is the New Weapon:** Disinformation campaigns, meme wars, and fake narratives can destabilize democracies and incite internal unrest.

### Hybrid & Asymmetric Warfare: Threats to India

- **Cross-Border Terrorism & Proxy War:** India faces a sustained asymmetric threat from Pakistan, which actively sponsors terrorism through groups like Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM).
- **Information Warfare and Psychological Operations:** India's internal cohesion is frequently targeted through deliberate disinformation campaigns, often amplified via social media. These operations aim to provoke communal unrest, manipulate political sentiment, and radicalize youth.
- **Cyberattacks on Critical Infrastructure:** India's growing digital infrastructure is increasingly under threat from cyber actors. Notably, the Kudankulam Nuclear Power Plant suffered a malware intrusion in 2019, and in 2020, the Mumbai power grid experienced a sudden blackout, which was later linked to suspected Chinese cyber operations.
- **Economic Warfare and Supply Chain Vulnerability:** India's economic dependencies, especially on China, expose it to strategic coercion. Nearly 80% of Active Pharmaceutical Ingredients (APIs) in Indian medicines come from China, creating a chokepoint during geopolitical tensions.
- **China's Grey-Zone Tactics and Territorial Encroachments:** China has perfected the art of grey-zone warfare — where actions fall just short of provoking open conflict. It employs tactics like "salami slicing" to gradually shift territorial realities, as witnessed during the 2020 Galwan clashes.
- **Digital Espionage and Surveillance Threats:** India's leadership, institutions, and strategic assets have been targets of digital surveillance. The Pegasus spyware controversy raised concerns about the potential misuse of advanced surveillance tools by both foreign and domestic players.

### India's Readiness for Modern, Asymmetric & Hybrid Warfare

- **Integrating Technology:** India recognizes the importance of multi-domain operations, integrating **AI-driven surveillance, cyber defense, and unmanned aerial systems** into its military framework.
  - ♦ The **Akashteer air defense system** has emerged as a key asset, providing real-time threat detection and automated response mechanisms.
- **Leveraging Unconventional Strategies:** The **DRDO Young Scientist Laboratory - Asymmetric Technologies (DYSL-AT)** is spearheading research into **AI-powered swarm algorithms** and **unmanned aerial vehicles**.
- **Addressing Multi-Dimensional Threats:** India has acknowledged the growing complexity of non-kinetic warfare, with parliamentary committees actively studying defense preparedness.
  - ♦ It has stressed the importance of collaborative security frameworks to counter hybrid threats.
  - ♦ Enhancing intelligence-sharing between military and government agencies to combat hybrid threats effectively.

### Conclusion

- Modern, asymmetric, and hybrid warfare redefine traditional combat, making conflicts more complex and unpredictable.
- India needs to adapt, innovate, and collaborate with its strategic allies to stay ahead in the evolving battlefield.
- India's focus on technological advancements and strategic preparedness ensures it remains resilient against emerging threats.

Source: BS

### Mains Practice Question

[Q] How effectively is India adapting to the evolving landscape of modern, asymmetric, and hybrid warfare, considering its technological advancements, military strategies, and geopolitical challenges?

