

# FROM CONVENTIONAL WARFARE TO GREY-ZONE CONFLICT

MS VAIBHAVI KATAL





## CENJOWS

### From Conventional Warfare to Grey-zone Conflict



**Ms Vaibhavi Katal** is a Research Assistant and Publication Head at CENJOWS

#### Introduction

Technological advancements have changed the way warfare is looked at in the 21st century. Traditionally, the battlefield has been viewed as a confrontation between state actors through systematic military strategies. Territorial gains, neutralisation of enemy combatants, and political repercussions determined the victor in a conflict. This influenced military operational guidelines, strategic planning and frameworks of national security around the world. Recent technological advancements have, however, made the traditional models of warfare outdated, as wars are now shifting away from tanks and troops.<sup>1</sup>

In the present-day battlefield, state as well as non-state actors participate in a diverse array of combat tactics that go beyond traditional warfare strategies. Though the classical models of warfare are obsolete, the conventional military forces that they relied on are still crucial for controlling territories, deterring enemy advances and action, and maintaining stability. Conflicts now employ information gathering, military planning, understanding of the economic landscape, ideological proficiency and technological know-how. The use of these frequently in tandem has blurred the boundary between ethical and unethical tactics. As a result, the barriers that traditionally divided various types of conflicts have become convoluted, making them difficult to identify.

This paper explores the transition from conventional warfare to grey-zone conflict by examining three essential dimensions. First, it discusses the characteristics and constraints of conventional warfare as the dominating paradigm. Second, it investigates the rise of hybrid warfare and grey-zone techniques as a key element for modern combat. Third, it investigates the role of sub-conventional warfare and its consequences for national security. This paper aims to explain why conflicts are no longer fought with only tanks and infantry but rather across several interrelated domains.

### **Conventional Warfare and Its Limitations**

Following India's independence, its security framework was largely dependent on conventional means of engaging in war. The conflicts of 1947-48, 1965, and 1971 with Pakistan, combined with the 1962 war with China, cemented a classic understanding of defence centred on maintaining territorial integrity and mobilisation of troops on a large scale. These wartime strategies required defined fighting zones with identifiable enemies and mobilisation of military troops. The strategic success of a conflict was dictated by territorial control, results of military operations and political will. These experiences emphasised the need for a state-centric, military-focused view of security in India's strategic thinking.

The 1962 confrontation with China brought to light the deficiencies in India's readiness to respond to such attacks, specifically in the logistics, infrastructure, and strategic planning departments.<sup>2</sup> The character of the conflict remained conventional, with the organised armed forces of both sides engaging in direct confrontation. The wars with Pakistan were fought with integrated land, air, and naval operations – more examples of traditional warfare. The subsequent victories against Pakistan, particularly the multi-domain success of 1971 that led to the creation of Bangladesh, solidified the belief that armed forces were the primary shield of the state. The trust in traditional military forces as the backbone of national security was bolstered by these experiences.<sup>3</sup>

The shortcomings of this framework became clear with time. The Kargil War of 1999, while fought on conventional lines, introduced severe geopolitical restrictions. While India achieved tactical triumph, the war emphasised the hazards of escalation in a nuclear environment. It also exposed that without launching a full-scale war, the vulnerabilities in surveillance and preparedness may be exploited.<sup>4</sup>

Since Kargil, India's national security issues have shifted away from conventional warfare. A system has formed in which threats are ongoing, owing to persistent cross-border terrorism, infiltration and proxy warfare, but seldom lead to open confrontation.<sup>5</sup> Conventional military dominance has little use in such cases. Various types of dangers require varied responses, and mobilisation of troops on a large scale for every situation is neither economically viable nor suitable. This has shed light on the limitations of a security framework largely dependent on classical battlefield engagements.

Furthermore, traditional warfare sets a distinct boundary between war and peace, combatants and non-combatants, and military and civilian spheres. India's current security situation calls these differences into question as threats evolve gradually, traversing boundaries, and involve both state and non-state actors. In such scenarios where prolonged, uncertain and scattered fighting is prevalent, emphasis on a conclusive victory becomes less important. Consequently, traditional tactics, while necessary, are insufficient to solve India's security concerns which cover a wide spectrum.

Shifting patterns of warfare have exposed the limitations of reliance on military might, and the growth in security experience has demonstrated the necessity to go beyond the conventional form of combat. A comprehensive and flexible approach must be taken to ensure that such modern challenges are addressed in a manner that synergises and enhances military capability with new frontiers of combat. This evolution provides the foundation for understanding the rise of hybrid, grey-zone, and sub-conventional forms of conflict, which largely characterise the contemporary security environment.

## **THE EMERGENCE OF HYBRID WARFARE**

The ever-evolving character of warfare has paved the way for what is now called 'hybrid warfare'. Unlike conventional warfare, which largely focuses on military might to achieve political goals, hybrid warfare integrates military and non-military tactics in a coordinated manner. It merges conventional operations with cyberattacks, narrative campaigns, economic coercion, proxy actors, and diplomatic manoeuvring to affect an adversary's conduct. The goal is not always to achieve a decisive tactical victory but to affect strategic outcomes while minimising the costs and risks that come with open conflict.<sup>6</sup>

The emergence of hybrid warfare indicates a larger realisation that power may be used across numerous areas at once. Modern battles are increasingly being waged not just on land, sea, and air, but also in cyberspace, the information environment, and economic networks.<sup>7</sup> This multimodal strategy enables governments to exploit vulnerabilities that traditional military strategies frequently ignore. Hybrid warfare combines many statecraft methods to build cumulative pressure that weakens an enemy over time rather than via a single decisive conflict.

The 2014 annexation of Crimea offers a clear study in hybrid operations. Instead of launching a frontal assault, Russia deployed a highly coordinated mix of unmarked personnel ("little green men") and local proxy militias; conducted heavy information operations; and engaged in political subversion. The ambiguity about the identity and role of the so-called "little green men" slowed international response and complicated attribution. Military power was there, but it was only one component of a larger plan aimed at shaping perceptions and altering ground realities before effective countermeasures could be implemented.<sup>8</sup>

The ongoing Russia-Ukraine war further demonstrates this hybrid evolution. Alongside high-intensity kinetic clashes, both sides actively weaponize cyber tools, control global media narratives, enforce economic sanctions, and execute aggressive diplomatic manoeuvring. The conflict has demonstrated that modern warfare is not limited to battlefields. Narratives, public perception, and technological skills have all become critical components of strategic competitiveness. Victory increasingly depends on the capacity to coordinate efforts across different domains, rather than just military superiority.<sup>9</sup>

Rather than launching outright military offensives, Beijing utilises an incremental mix of economic leverage, legal warfare (the three warfare's doctrine), media manipulation, rapid infrastructure building, and grey-hulled maritime militia coercion.<sup>10</sup> Such strategies allow for incremental changes to the status quo while remaining below the threshold that generally triggers a military reaction. This calibrated use of power exemplifies how hybrid techniques may be used during both peace and crisis.

For India, the importance of hybrid warfare stems from the awareness that current security challenges are rarely isolated to a single area. Cross-border terrorism, cyber incursions, spread of misinformation, and economic dependence can all work together to generate stresses that traditional military solutions alone cannot alleviate. The emergence of hybrid warfare calls into question traditional security thinking and necessitates a more integrated strategy that blends military readiness with informational, technical, diplomatic, and economic capabilities. Understanding this change is critical for evaluating the increasingly ambiguous forms of conflict that define the modern security environment.

### **Grey-Zone Tactics and Strategic Ambiguity**

Grey-zone conflict falls in between typical statecraft and conventional combat. It entails coercive competitive actions that are purposely kept below the level of open armed combat. The primary goal is to achieve strategic benefits while avoiding a significant military reaction from the adversary.<sup>11</sup> Grey-zone tactics are based on ambiguity, deniability, and incrementalism, making it hard to judge if the hostile conduct deserves escalation. In many respects, grey-zone conflict contradicts the long-held binary divide between war and peace in strategic thought.

In the Indian context, China's actions along the Line of Actual Control (LAC) are one of the most obvious examples of grey-zone tactics. Rather than participating in large-scale military offensives, China has frequently used gradual territorial claims, infrastructural development, strategic patrols, and coercive signals to change ground realities.<sup>12</sup> The 2017 Doklam standoff and the 2020 Galwan Valley clashes were sharp reminders of this strategy: reshaping ground realities without triggering a full-scale regional war. Such events take advantage of uncertainty by remaining important enough to confront India's interests while being calibrated enough to avoid conventional military escalation.

Pakistan's long-standing dependence on proxy wars and cross-border terrorism exhibits features of grey-zone strategy. While terrorist acts fall under the category of sub-conventional combat, their greater strategic usefulness is in putting pressure on India while preserving varied degrees of deniability. This creates a situation in which attribution may be politically clear but legally challenged, limiting reaction choices.<sup>13</sup>

The goal is not to conquer territory but to create long-term instability and strategic diversion.

The undeniable fact about the grey-zone techniques is that they make us address the shortcomings of traditional dissuasion. When rivals avoid direct conflict, military might lose effectiveness to a large extent. Responding with force may look unreasonable in such situations, while tolerance may be taken as weakness and promote further coercive action. This generates a strategic dilemma in which countries must walk a tightrope to determine suitable reaction thresholds.

The undeniable fact about the grey-zone techniques is that they highlight the shortcomings of conventional deterrence. When rivals avoid direct conflict, conventional military dominance becomes less effective. Responding with overwhelming force may look unreasonable, yet forbearance may promote further coercive action. This generates a strategic quandary in which countries struggle to determine suitable reaction thresholds.

For India, grey-zone conflicts highlight the need for a broader vision of security that stretches beyond military preparation. Intelligence gathering, diplomatic engagement, economic resilience, information management, and military preparation are all necessary components for effective responses to such multi-pronged conflicts. The aim is to go beyond simply avoiding conflict to preventing opponents from making strides through sustained pressure. With rivalries moving below the threshold of open war, detecting and responding to grey-zone tactics has become an important component of modern security frameworks.

### **Sub-Conventional Conflict and Proxy Warfare**

Sub-conventional conflict lies between conventional war and peacetime struggle. It includes the use of techniques like sponsored terrorism, proxy wars, infiltration, and covert operations to inflict costs on an enemy while avoiding full-scale military combat.<sup>14</sup> Pakistan's long-standing utilisation of cross-border terrorism against India is one of the most notable examples of unconventional conflict. Such techniques attempt to take advantage of the limits imposed by nuclear deterrence, allowing the persistence of hostile acts below the threshold of conventional conflict and granting varied degrees of deniability.

The persistence of the problem can be observed when analysing India's history since the late 20th century. High-profile operations like the 2001 Parliament attack and the 2008 Mumbai attacks proved that a small group of non-state actors with high deniability could achieve massive strategic and political leverage.<sup>15</sup> Such attacks harm not just lives and infrastructure but also damage public trust and government power. The attacks aimed to be and were successful in creating long-term uncertainty and strategic pressure and did not aim to acquire territory. The limitations of traditional military power were revealed when confronted with such dispersed and irregular forms of warfare.

A critical shift in India's sub-conventional response strategy was seen during the 2019 Pulwama attack. India's retaliatory airstrikes deep within the enemy camps at Balakot moved away from purely diplomatic and strategic containment, fundamentally recalibrating the deterrence equation.<sup>16</sup> This answered the need to overhaul the existing deterrence dynamics and escalation assumptions. The contrast between the attacks at Parliament and Mumbai and the response to Pulwama reveals how sub-conventional combat strategies have become a permanent aspect of India's security environment, successfully bridging the gap between traditional warfare and the nuances of modern conflict dominated by larger hybrid and grey-zone operations.

### **Technology and the Transformation of Conflict**

The nature of modern combat has been fundamentally transformed by technological breakthroughs and has led to the inclusion of cyberspace, outer space, and the information space into the present-day battlefield.<sup>17</sup> Technology has opened up avenues for governments and non-state actors to achieve their strategic goals, despite the armed forces remaining an essential instrument of state power. The gradual shift of society from analogue to digital, with an increased reliance on digital networks, communication systems, and data infrastructure, has inadvertently created weakness that may be exploited without the use of conventional warfare strategies. As a result, technological capabilities are increasingly shaping the battlefield in addition to traditional military might.

The rise of the digital space as a front of strategic rivalry due to advancements in technology and increased dependence on them has been one of the most significant changes in defining the modern battlefield. Cyber operations can, without crossing

physical boundaries, compromise sensitive information, destroy key infrastructure, and interfere with government and military systems.<sup>18</sup> Unlike traditional attacks, cyberattacks are difficult to attribute, allowing malevolent actors to operate with an increased degree of anonymity. The effectiveness of a few lines of code being the same as a wing of fighter bombers was proved by the historic Stuxnet operation against Iran's nuclear infrastructure, modifying the traditional deterrence paradigm at its core. Such innovations have increased the avenues present for governments to carry out operations, challenging the existing deterrence framework.<sup>19</sup>

Technology has also changed the purpose of information in warfare. The dissemination of misinformation has been accelerated due to social media platforms, digital communication networks, and technologies employing artificial intelligence. Contemporary wars are increasingly accompanied by debates about narratives, public image, and legitimacy. The conflict between Russia and Ukraine has demonstrated the effectiveness of misinformation campaigns, digital mobilisation, and real-time communication in impacting both domestic and international audiences. The control over a narrative, in this context, becomes as strong and important as control over a territory.<sup>20</sup>

For India, technological development creates both opportunities and problems. Economic development and governmental capability have been boosted by the rapid digitisation of systems, but it has also made the very systems vulnerable to cyberattacks, misinformation operations, and technological coercion. Artificial intelligence, autonomous systems, and space-based capabilities are increasingly gaining importance and altering military strategic approaches. Consequently, national security can no longer be understood only through the microscope of territorial defence. The capability to defend digital infrastructure, preserve informational ecosystems, and respond to technological change has become a vital component of modern security strategy, reflecting the changing nature of warfare in the twenty-first century.

## **Conclusion**

The evolution of warfare from direct military confrontations to hybrid, grey-zone, and technology-enabled forms of conflict has resulted in a fundamental transformation in the manner in which power is exercised in contemporary international politics. While

conventional warfare instruments like tanks, aircraft, and military personnel remain important to statecraft, they can no longer be considered the sole determinants of strategic success. States increasingly pursue their objectives through combined military and non-military operations, including but not limited to employing misinformation campaigns, utilising cyber capabilities, creating economic pressure, sponsoring proxy actors, and creating strategic ambiguity to shape outcomes. Consequently, the distinction between war and peace has become increasingly blurred, leading to persistent security challenges that are multidimensional in nature and often harder to attribute.

This shift has far-reaching implications for India's defence strategy. In addition to conventional military threats, cross-border terrorism, grey-zone coercion, narrative manipulation, and the ability to identify and minimise technological weaknesses all influence the country's security situation. Rising concerns can no longer be dealt with by traditional security systems, which were largely created for interstate combat between military forces. To create a stronger and more resilient security framework, greater integration of military, diplomatic, technical, economic, and information realms is necessary. Policies must, therefore, be designed with an emphasis on adaptability to the changing nature of warfare and an understanding of the modern geopolitical climate while also protecting India's interests in an era where wars are fought as much using influence, information, and technology as through force.

### **Declaration**

I declare that this manuscript is being submitted exclusively to CENJOWS for publication consideration, is original, and has not been published or submitted elsewhere. I further certify that it contains no classified, restricted, or sensitive information and is based entirely on open-source material suitable for publication in the public domain.

## ENDNOTES

- <sup>1</sup> Bhattacharjee, Subimal. "The Evolution of Modern Warfare: How Technology Is Transforming the Rules of War." <https://www.natstrat.org>, 2025. <https://www.natstrat.org/articledetail/publications/the-evolution-of-modern-warfare-how-technology-is-transforming-the-rules-of-war-212.html>
- <sup>2</sup> Lovell, Shivom Singh. "The 1962 Sino-Indian War Was a Brief but Intense Clash, Fought Ostensibly over Disputed Himalayan Borders. Before 1949, India and China Shared No Common Boundary at All, Making the Idea of a Border Dispute Impossible." <https://www.linkedin.com/pulse/essay-1962-sino-indian-conflict-shivom-singh-lovell-obn5f/>
- <sup>3</sup> Chaya, Dheeraj Paramesha. "The Fundamental Principles of Covert Military Action: Lessons from India's 1971 Experience." [orfonline.org](https://www.orfonline.org/research/the-fundamental-principles-of-covert-military-action-lessons-from-india-s-1971-experience). OBSERVER RESEARCH FOUNDATION ( ORF ), June 25, 2024. <https://www.orfonline.org/research/the-fundamental-principles-of-covert-military-action-lessons-from-india-s-1971-experience>
- <sup>4</sup> Bommakanti, Kartik. "Coercion and Control: Explaining India's Victory at Kargil." *India Review* 10, no. 3 (July 2011): 283-328. <https://doi.org/10.1080/14736489.2011.596787>
- <sup>5</sup> Shukla, Shruti. "'Cross Border Terrorism' Examining the India- Pakistan Relationship." *International Journal of Novel Research and Development* 9 (March 3, 2024): 405. <https://www.ijnrd.org/papers/IJNRD2403648.pdf>
- <sup>6</sup> Hoffman, Frank. "Conflict in the 21st Century: The Rise of Hybrid Wars." Potomac Institute for Policy Studies, 2007. [https://www.potomac institute.org/images/stories/publications/potomac\\_hybridwar\\_0108.pdf](https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf)
- <sup>7</sup> Bingen, Kari A. "Welcome to Zscaler Directory Authentication." [Csis.org](https://www.csis.org/analysis/chapter-8-extending-battlespace-space), September 16, 2025. <https://www.csis.org/analysis/chapter-8-extending-battlespace-space>
- <sup>8</sup> *ibid*
- <sup>9</sup> Biegon, Rubrick, Daniel Møller Ølgaard, and Tom F.A. Watts. "Interrogating the Imaginary Turn: Technology, War, and World Politics in an Era of Great Power Competition." *Contemporary Security Policy* 47, no. 2 (March 2, 2026): 241-72. <https://doi.org/10.1080/13523260.2026.2638846>
- <sup>10</sup> ANI. "China's Hybrid Warfare Escalates as Beijing Expands Maritime Pressure on Taiwan." ANI News, June 21, 2026. <https://www.aninews.in/news/world/asia/chinas-hybrid-warfare-escalates-as-beijing-expands-maritime-pressure-on-taiwan20260621185932/>
- <sup>11</sup> Shinde, Col Vikrant S. "Deciphering the Grey Zone - Takshashila Institution." [Takshashila.org.in](https://takshashila.org.in/content/publications/20251014-Deciphering-the-Grey-Zone.html), October 14, 2025. <https://takshashila.org.in/content/publications/20251014-Deciphering-the-Grey-Zone.html>
- <sup>12</sup> Dave, Aaditya. "India-China Clashes: Escalation along the Line of Actual Control." [Rusi.org](https://www.rusi.org/explore-our-research/publications/commentary/india-china-clashes-escalation-along-line-actual-control), June 18, 2020. <https://www.rusi.org/explore-our-research/publications/commentary/india-china-clashes-escalation-along-line-actual-control>
- <sup>13</sup> Bains, Hrishik. (2026). Grey Zone Warfare in South Asia: India's Strategic Response to Pakistan's Proxy Strategy. 10.13140/RG.2.2.25260.63363
- <sup>14</sup> Dixit, K.C. "Sub-Conventional Warfare Requirements, Impact and Way Ahead," n.d. [https://idsa.in/system/files/jds\\_4\\_1\\_kcdixit.pdf](https://idsa.in/system/files/jds_4_1_kcdixit.pdf)
- <sup>15</sup> Suryawanshi, Shweta. "Politics, Media, and Terrorism: Understanding the Discourse Surrounding the 2001 Attack on Indian Parliament," 2019. [https://cjids.in/wp-content/uploads/2026/05/CJIDS\\_V3\\_Politics-Media-Terrorism\\_2001-Indian-Parliament-Attack.pdf](https://cjids.in/wp-content/uploads/2026/05/CJIDS_V3_Politics-Media-Terrorism_2001-Indian-Parliament-Attack.pdf)
- <sup>16</sup> Noor, Sitara. "Pulwama/Balakot and the Evolving Role of Third Parties in India-Pakistan Crises • Stimson Center." Stimson Center, March 25, 2020. <https://www.stimson.org/2020/pulwama-balakot-and-the-evolving-role-of-third-parties-in-india-pakistan-crises/>
- <sup>17</sup> Singh, Tejinder. "Evolution of Multi-Domain Operations and Prospects for Application of Aerospace Power." *Manohar Parrikar Institute for Defence Studies and Analyses Journal of Defence Studies* 18, no. 1 (2024): 67-87. [https://www.idsa.in/wp-content/uploads/2024/05/18-1\\_Tejinder-Singh.pdf](https://www.idsa.in/wp-content/uploads/2024/05/18-1_Tejinder-Singh.pdf)
- <sup>18</sup> *ibid*
- <sup>19</sup> Harshad Katikar. "Stuxnet-Analysis and Implications of the World's First Cyber-Weapon." ResearchGate, August 16, 2024. <https://doi.org/10.13140/RG.2.2.10847.27043>
- <sup>20</sup> Divon, Tom, and Moa Eriksson Krutrök. "The Rise of War Influencers: Creators, Platforms, and the Visibility of Conflict Zones." *Platforms & Society* 2 (March 2025). <https://doi.org/10.1177/29768624251325721>