

Non-Contact and Non-Kinetic Warfare in the Indian Context: Concepts and Pathways

Colonel Vikram Tiwari[@]

“The future of conflict will not be fought in trenches or skies, but in the minds and hearts of people”

- Shri S Jaishankar, External Affairs Minister of India

Abstract

The essay examines the evolving paradigm of non-contact and non-kinetic warfare within the Indian context, highlighting its critical relevance in the age of 5th generation warfare. It explores historical precedents, current challenges posed by adversaries like China and Pakistan, and the growing role of cyber, information, space, and psychological warfare in shaping modern conflict. Through a detailed analysis of India's threat landscape, the essay outlines strategic pathways for integrating non-contact and non-kinetic domains into the national security architecture. The essay concludes with a call for holistic, proactive, and coordinated national efforts to secure India's interests in an increasingly contested and interconnected world.

Introduction

The evolution of warfare has transcended traditional battlegrounds, moving beyond physical confrontations to embrace non-contact and non-kinetic strategies. The adoption of

This is the Second Prize winning entry of the USI Gold Medal Essay Competition.

[@]**Colonel Vikram Tiwari** is a serving officer of the Corps of Signals with extensive operational and staff experience. Over the course of his career, he has served in signals regiments across diverse sectors, gaining wide exposure in communications and operational support. He has commanded a Mountain Divisional Signal Regiment deployed along the Northern Borders, demonstrating leadership in high-altitude operational environments. His staff appointments include a tenure with the Acquisition Wing of the Ministry of Defence, where he contributed to capability development and procurement processes. A graduate of the Higher Defence Management Course, he has also served as an Instructor at the Army War College.

Journal of the United Service Institution of India, Vol. CLV, No. 641, July-September 2025.

these strategies by state and non-state actors has led to disproportionate successes with minimal resource commitment by the initiators, thereby, rendering these approaches of significant importance in the evolving landscape of modern conflict. The additional attribute of plausible deniability offered by this form of warfare makes it an even more attractive option for subtle yet impactful strategic signalling and power projection. For nations, like India, which face multifaceted security challenges, non-contact and non-kinetic forms of warfare need to be recognised as a major security threat. There is an urgent and inescapable requirement to incorporate effective measures to counter and mitigate their effects, while simultaneously developing credible capabilities to leverage them against adversaries as part of the national security strategy.

Non-contact warfare refers to tactics that do not require physical presence or direct engagement with the adversary. Non-kinetic warfare, on the other hand, involves methods that do not rely on conventional kinetic force. Both, often encapsulated within the framework of 5th Generation Warfare (5GW), represent a paradigm shift in conflict. The rise of digital technologies and global connectivity has amplified the impact of these tactics. Unlike traditional warfare, which relies on physical force and direct engagement, 5GW leverages information, cyber capabilities, and psychological operations to achieve strategic objectives without direct confrontation. This form of warfare is characterised by its focus on influencing perceptions, disrupting societal norms, undermining trust in institutions through sophisticated means such as misinformation campaigns, cyber campaigns, and social engineering besides leveraging cyber-attacks to disrupt critical infrastructure. As nations and non-state actors increasingly adopt these methods, the battlefield extends beyond physical territories into the realms of cyberspace and public consciousness. Effective national security in the age of 5GW requires a holistic, adaptive approach and seamless coordination to address these multifaceted threats.^{1,2}

Historical Context of 5th Generation Warfare in India

India's Legacy in 5GW. India's historical experience, from ancient statecraft to modern-day conflicts, illustrates the gradual evolution of warfare towards the principles that define 5GW today. India's

history provides rich examples of how non-traditional forms of warfare (now termed as 5GW) have been and continue to be a critical aspect of the nation's strategic landscape. Understanding the historical context and evolving nature of non-contact and non-kinetic warfare is crucial for comprehending the complexities of contemporary conflicts and preparing for future challenges in an interconnected world.

***Arthashastra* (The Science of Statecraft) and Early Forms of Psychological Warfare.** One of the earliest references to what could be considered a precursor to 5GW is found in the *Arthashastra*, outlining covert operations like espionage, propaganda, and psychological tactics to weaken enemies. Chanakya's strategies in unifying India under Chandragupta Maurya involved diplomacy, alliances, and subversion, which are key elements of modern 5GW, focusing on influencing adversaries without direct confrontation.³

Medieval India: The Marathas and Asymmetric Warfare. In the 17th and 18th Centuries, the Maratha Empire offered another historical perspective on the evolution of warfare strategies that resonate with 5GW concepts. The Marathas, under Shivaji, employed guerrilla tactics to disrupt and exhaust the Mughal forces. Their strategy of mobility, surprise, and local terrain knowledge reflects the non-linear, decentralised tactics of 5GW, emphasising indirect confrontation with stronger foes.

Modern Era: Insurgencies and Proxy Wars. Post-independence, India faced 4th generation warfare through insurgencies in Punjab, Kashmir, and the North-East, marked by proxy wars and terrorism fuelled by Pakistan and China. These conflicts, where non-state actors played a significant role, have been marked using civilian violence, terrorist acts, associated propaganda, and the manipulation of local populations.⁴

Early 21st Century: Cyber Threats, Information Warfare (IW), and Social Engineering. By the early 21st Century, as India became increasingly integrated into the global digital ecosystem, cyber warfare and information operations emerged as significant concerns, with instances of cyber espionage and the spread of misinformation aiming to disrupt India's political and economic stability. With the widespread prevalence of social media, the associated spread of disinformation through social media platforms

emerged as a significant concern in India. These threats have assumed increasing relevance in an interconnected world.

Concepts of Non-Contact and Non-Kinetic Warfare

Modern Forms of Warfare. Non-contact and non-kinetic warfare represent modern approaches to conflict that diverge from traditional and direct military engagements. Non-contact warfare emphasises strategies where physical confrontation is minimised or avoided altogether. This form of warfare leverages technology, cyber capabilities, and information operations to achieve objectives without the need for conventional force deployment. Non-kinetic warfare, on the other hand, involves methods that do not rely on physical force to achieve strategic goals. The intent is to undermine the opponent's decision-making processes, morale, or infrastructure without direct physical impact. Both forms of warfare reflect the changing nature of conflict in the 21st Century, where the boundaries between peace and war blur, and the focus shifts to influence and disruption rather than outright destruction.⁵⁶

Dimensions of Non-Contact and Non-Kinetic Warfare. Non-contact warfare encompasses a variety of strategies designed to engage an adversary without direct physical confrontation. Key constituents include cyber warfare, which involves hacking, cyber espionage, and cyber-attacks to disrupt critical infrastructure and communication networks. Electronic Warfare (EW) is another critical component, targeting the enemy's radars, communications, and navigation systems to gain a strategic advantage. Additionally, information operations, including psychological operations, are employed to manipulate perceptions and influence the morale of the opposing force. On the other hand, non-kinetic warfare includes elements of cyber and IW besides new domains of conflict i.e., utilising economic, diplomatic, and legal statecraft to achieve strategic objectives. IW is a significant constituent, utilising propaganda, media manipulation, and disinformation to control narratives and influence public opinion along with psychological operations aimed at eroding the enemy's will to fight by targeting their decision-making processes, leadership, and societal cohesion.

Hybrid and Grey-Zone Operations. Hybrid and grey-zone warfare represent complex and evolving strategies within the broader framework of 5GW, characterised by the integration of conventional and unconventional tactics to achieve strategic objectives in a

manner that blurs the lines between war and peace. These approaches exemplify the shift away from traditional warfare towards more nuanced and multifaceted methods of conflict, where the focus is on influence, disruption, and subversion rather than direct military engagement.

Hybrid Warfare. Hybrid Warfare seeks to exploit the vulnerabilities of an adversary by blending traditional military operations with non-traditional methods to create a more comprehensive and unpredictable strategy. It aims to achieve strategic objectives by integrating various forms of power to confuse, destabilise, and ultimately subdue an opponent without necessarily engaging in full-scale combat.⁷

Grey-Zone Warfare. Grey-zone warfare operates in the ambiguous space between traditional warfare and peace, where actions fall below the threshold of conventional conflict and are often characterised by their ambiguity and indirectness. Grey-zone tactics include cyber espionage, political subversion, economic sanctions, and the strategic use of proxy forces. The goal is to achieve strategic gains while avoiding overt conflict and maintaining plausible deniability. This strategy involves the use of economic leverage, legal arguments, and incremental territorial expansion to achieve strategic goals without provoking an all-out military response.⁸

Challenges in the Indian Context

India's Strategic Landscape. This is characterised by its geostrategic compulsions and complex security environment. With hostile neighbours like Pakistan and China, and internal security challenges, India faces a range of threats across the wide spectrum of conflict, from non-contact and non-kinetic realms to nuclear domain that require innovative and multifaceted responses.

Indian Security Concerns in the Era of 5GW. India's main adversaries i.e., Pakistan and China, are considered masters of 5GW. Pakistan's focussed approach towards IW was primarily driven by its early realisation that it was up against a much more powerful adversary but one with diverse ethnicity, faiths, regions, and linguistics, all of which could be exploited to weaken it. China embarked on conceptualising the doctrine of 'War under conditions of informationalisation' relatively early in 1993. Anticipating the

rapid rise in information and communication technology, China invested in transformational change to its war-fighting doctrines, adopting the strategy of Three Warfares i.e., Media, Legal, and Cyber. China is adopting concepts to contribute to hybridity through 'Wolf Warrior' diplomacy, aggressive political posturing, and legal warfare, with the latest border laws being a subset of the latter. With India, border coercion mixed as a low-level conventional threat with 5GW is likely to remain its strategy.⁹

Cyber Warfare. India, as an emerging global power and a significant stakeholder in digital transformation, faces increasing threats in the cyber domain. These threats range from state-sponsored cyber espionage to attacks on critical infrastructure, aiming to disrupt the nation's economic, military, and governmental functions. Notable incidents, such as the 2012 cyber-attacks on Indian government websites and the alleged Chinese cyber intrusions targeting India's power grid in 2020, underscore the growing relevance of cyber defence. These attacks highlight vulnerabilities in India's cyber infrastructure and the potential ramifications of cyber-attacks on national security. The range and scope of cyber-attacks have increased manifolds. The persistent and evolving nature of cyber threats emphasise the need for robust cybersecurity measures to protect the nation's critical infrastructure and data.¹⁰

Information Warfare.

- **EW.** This plays a crucial role in the evolving landscape of Cyber and ElectroMagnetic Activities (CEMA) dominating future battlespace. Both Pakistan as well as China have significant EW capabilities. The situation assumes additional gravity in the likely collusivity scenario.
- **Information Operations.** India faces significant challenges in this domain, owing to its diverse religious, ethnic linguistic, and cultural fault lines. Pakistan and China have on numerous occasions attempted to exploit these through propaganda, disinformation, and psychological operations to shape narratives and destabilise internal security. IW, through the realms of psychological warfare and social engineering, necessitates robust countermeasures to protect national security and societal cohesion. Its evolving nature—such as

the rise of deepfakes and artificial intelligence-generated content, which complicate the information landscape—presents fresh challenges. As information becomes increasingly weaponised, India's approach to IW needs to not only defend against these threats but also to proactively shape narratives that support national security objectives.¹¹

Space Warfare. India has made rapid strides in space-based technologies. Owing to its image as a peaceful democracy and its rapid economic and technological growth, India has emerged as a preferred choice for many developing countries for partnership in the field of space technologies. India's growing dependence on space-based systems for both civilian and military applications make the protection of these assets a strategic priority. The rise of China's space capabilities, including its demonstrated ability to target satellites, has heightened India's concerns about the potential for space to become a new domain of conflict. In this scenario, space-based warfare assumes increasingly vital importance from an Indian perspective. The successful execution of Mission SHAKTI in 2019, where India tested its own Anti-Satellite (ASAT) weapon, was a clear response to these emerging threats, signalling India's resolve to defend its space assets against potential adversaries. As space becomes increasingly contested, India's approach to space warfare is crucial for maintaining strategic deterrence and ensuring the security of its space-based assets without engaging in direct conflict.¹²

Economic Coercion, Diplomatic Manoeuvring, and Legal Warfare. These are vital components of non-contact and non-kinetic warfare, with profound implications for India's strategic autonomy and national security. As an emerging global power, India has the capacity and the capability to actively engage in these domains to assert its interests while safeguarding its sovereignty.

Challenges in the Domains of Hybrid and Grey-Zone Warfare

Hybrid Warfare. This poses intricate challenges for India. These tactics exploit vulnerabilities within India's diverse society, particularly in a geopolitical environment marked by tensions with Pakistan and China. Pakistan's use of proxy groups to sponsor terrorism in Jammu and Kashmir, coupled with disinformation campaigns aimed at inciting unrest, exemplifies hybrid warfare in

its true context. Similarly, China's cyber intrusions targeting Indian infrastructure and its economic coercion through trade policies illustrate the multifaceted nature of this threat. To counter hybrid threats, India must continuously update its strategies and strengthen internal mechanisms. Efforts like the abrogation of Article 370 to curb separatist sentiments have been a major game changer. These need to be sustained, and a pro-active stance would reap substantial dividends.¹³

Grey-Zone Warfare. Grey-zone warfare seeks to exploit ambiguities while avoiding full-scale conflict. China's salami-slicing tactics in the Himalayas and Pakistan's use of non-state actors for cross-border skirmishes while officially denying involvement typifies the deniable characteristic of this warfare. The difficulty of attributing these non-military actions often leaves India in a reactive posture, struggling to craft responses that deter aggression without escalation. To counter these, India needs to undertake measures like enhancing border infrastructure and engaging in diplomatic efforts to isolate Pakistan internationally, while strengthening its internal security apparatus and public awareness campaigns to counter disinformation.¹⁴

India's Threat Landscape. The advent of 5GW amplifies the complexity of India's national security challenges. The ongoing proxy war with Pakistan and the tensions with China along its northern borders highlights the mix of conventional threats with various forms of non-contact and non-kinetic warfare including cyber-attacks, IW, and proxy conflicts. Adding to this mix, a substantial degree of hybrid and grey-zone tactics by its adversaries renders the security environment extremely volatile for India. Addressing such a threat landscape requires strategic policy shift to align the nation to its new security challenges and develop robust countermeasures and appropriate capabilities.

Potential Pathways for Integration

India's Response to Non-Contact and Non-Kinetic Warfare. As the global security landscape continues to evolve, traditional forms of warfare are increasingly complemented, and in some cases, replaced by non-contact and non-kinetic warfare. In this scenario, effectively dealing with non-contact and non-kinetic warfare threats is critical for India to ensure its national security and advancing its interests on the world stage. Potential pathways

and recommendations for building resilience against these threats while leveraging the same to further own national interests in key domains of non-contact and non-kinetic warfare are covered below:

- **Cyber Warfare.**

- Central agencies like the National Cyber Security Coordinator and the Indian Computer Emergency Response Team should be empowered with the latest tools and technologies to detect, prevent, and respond to cyber threats.
- Adequate investment in advanced research and development in the domain of cyber security.
- Leverage the extensive talent pool of young cyber professionals and freelancers to foster innovation through public-private partnerships.
- Strengthen digital sovereignty through initiatives like *Atmanirbhar Bharat* (Self-reliant India) to reduce dependence on foreign technology and retain control over critical cyber infrastructure.
- Collaborate with global partners in intelligence sharing and conducting joint cyber exercises to further bolster cyber defence.

Strategic Offensive Capabilities. Development and maintenance of robust offensive cyber capability, capable of striking back at adversaries, will serve as a powerful deterrent. This involves not only the creation of dedicated cyber organisations with clear mandate and development of advanced hacking tools and techniques but also the establishment of clear doctrines and rules of engagement for cyber warfare.

Information Warfare.

- **Information Operations and Strategic Communication.**

- Recognise information operations as an integral operational domain, where dominance is indispensable for achieving success. In many cases, shaping perceptions may be as crucial, if not more, than achieving operational success.

- Maintain the strategic communication initiative by proactively deploying own narratives in a timely manner, rather than responding reactively to adversary's propaganda, disinformation, or fake narratives.
- Develop specialised units, both civilian and military, at the national, strategic, and theatre levels to undertake proactive information campaigns that align with own objectives.
- Develop structures and systems to detect and counter-act against disinformation campaigns. These are to be equipped with advanced tools for tracking the spread of disinformation and deploying counter-narratives.
- Undertake public awareness campaigns and media literacy programs to empower citizens to recognise and resist disinformation.
- Harness the power of the nation's vast netizen youth, particularly influential social media voices, to amplify strategically crafted narratives and secure advantage in the battle of perceptions.
- Leverage India's soft power including its global diaspora, industry and technology leaders, cultural ambassadors, and rich civilisational heritage rooted in democratic values to project strategic narratives globally and effectively counter adversarial propaganda.

Enhancing EW Capabilities.

- Integrate EW capabilities of respective services through joint commands to ensure a unified approach to electronic threats.
- Acquisition of advanced EW systems for modernisation of armed forces.
- Focused investment in research and development efforts for developing indigenous EW systems through collaboration between Defence Research and Development Organisation, private industry, and academic institutions to reduce dependency on foreign technology.

CEMA. CEMA represents the convergence of cyber and EW, creating a comprehensive approach to dominate the electromagnetic spectrum and cyberspace. CEMA allows for synchronised and effective approach to not only enhances India's multi-domain advantage but also ensures a more resilient defence against emerging threats.

- **Space-Based Warfare.**

- **Leveraging Space Capabilities.** As space-based assets become more integral to national security, the need to protect them from adversarial actions has grown. Following aspects need prioritisation:

- o Enhance real-time space-based Intelligence, Surveillance, and Reconnaissance (ISR) capabilities and integrate with terrestrial and aerial ISR assets to enhance battlefield transparency.
- o Strengthen space-based communication and navigation systems to ensure secure, resilient, and uninterrupted support for military operations across all domains, including contested and denied environments.
- o Development of indigenous space industry for sustainability and independence of space program. Develop indigenous capabilities to reduce dependency on foreign technologies and supply chains.
- o Explore dual-use technologies to serve both civilian and military purposes.

- **Counter Space-Based Threats.**

- o Enhance space situational awareness, crucial for the safety and security of space assets, given the increasing congestion in space and the potential for collisions. Collaborate with international space agencies and private sector entities to timely detect and track potential threats, enabling pre-emptive measures to avoid or mitigate risks.

- o Refine ASAT capabilities, focusing on both kinetic (missile-based) and non-kinetic (cyber, EW) methods to act as a deterrent against adversaries.
- o Focus on enhancing the resilience of satellite infrastructure by implementing advanced encryption, hardening against electronic attacks, and ensuring redundancy through deployment of backup satellites. Additionally, explore use of small satellite constellations that are less vulnerable to single-point failures and can quickly replace any lost capability.
- o Incorporate space-based missile defence by integrating space-based sensors capable of detecting and tracking ballistic missile launches in real time for early warning and tracking data to ensure timely and effective response.
- o Engage in space diplomacy and collaboration to enhance own capabilities. Actively participate in international space forums and treaties to promote norms of responsible behaviour in space, including the prevention of space weaponisation and the management of space debris.

Economic Warfare.

- **Utilising Economic Statecraft.** As a rising economic power, India holds significant potential to leverage economic statecraft as a strategic tool. By employing targeted sanctions, trade policies, and investment strategies, India can execute punitive measures while effectively countering adversarial influence. Additionally, strategic investments in infrastructure and development projects enable India to expand its sphere of influence and foster long-term alliances to safeguard its national interests.
- **Promoting Economic Security.** India needs to focus on strengthening its economic resilience by diversifying supply chains, reducing dependency on foreign goods and technologies, and investing in critical industries like technology, defence, and energy. India should continue to promote self-reliance through initiatives like *Atmanirbhar Bharat*, as they aim to enhance domestic production and reduce vulnerability

to external economic pressures. By building strategic reserves of critical resources, investing in renewable energy, and fostering innovation in key industries, India can reduce its exposure to global economic shocks and enhance its strategic autonomy.

Diplomatic Manoeuvres.

- **Strengthening Diplomatic Networks.** In a multipolar world, where the balance of power is constantly shifting, India should continue to bolster its presence in international organisations, such as the United Nations and the World Trade Organization, and regional alliances like the grouping of Brazil, Russia, India, China, and South Africa, and the Quadrilateral Security Dialogue, to influence global norms and protect its national interests. India should strengthen strategic ties through bilateral and multilateral engagements, while engaging in diplomatic efforts for building coalitions to address common threats, such as terrorism, climate change, and cyber threats.
- **Diplomacy as a Deterrent.** Effective diplomacy can serve as a deterrent to adversaries by demonstrating a nation's ability to mobilise international support and isolate those who threaten its interests. By positioning itself as a responsible global power committed to peace and stability, India can enhance its diplomatic leverage and deter adversaries from pursuing aggressive actions.

Legal Warfare.

- **Leveraging International Law.** In an increasingly rule-based international order, legal warfare has become a critical tool for states to achieve strategic objectives and protect their interests. India should aggressively leverage international law as a tool of statecraft. This includes challenging the inimical actions in international courts and advocating for legal norms that protect its interests.
- **Defending National Interests.** India should actively advocate for the establishment of international legal frameworks governing emerging domains like cyber and space warfare, and ensure that its core concerns are addressed in legal frameworks, so that it has the legal tools to challenge adversaries who engage in aggressive actions.

Conclusion

Non-contact and non-kinetic warfare are becoming increasingly important in the modern strategic landscape. While India adapts to these multifaceted threats, the integration of these strategies into a comprehensive national security framework is essential. By enhancing its capabilities in cyber, space, and information operations domains, and leveraging its existing capabilities in economic statecraft and diplomatic engagement while formulating comprehensive policies, India can not only safeguard its sovereignty but also assert its influence in the region. As technology continues to evolve and the nature of warfare changes, India's ability to adapt and innovate will be crucial. With the right investments and strategic initiatives, India has the potential to lead while ensuring its security and sovereignty in an increasingly interconnected and contested world. The path forward requires a blend of technological innovation, strategic foresight, and robust international collaboration to ensure that India remains resilient and proactive in securing its national interests.

Endnotes

¹ Brigadier Vivek Verma, "Non-Contact Warfare (NCW): Managing Conflict in the 21st Century", *United Service Institution of India Journal* 149, no. 615 (Jan–Mar 2019), accessed 25 Jun 2025.

² Institute for Defence Studies and Analyses, *Hybrid Warfare: The Changing Character of Conflict*, edited by V. Deshpande, (New Delhi: Pentagon Press, 2018).

³ Ibid.

⁴ Lt Gen Syed Ata Hasnain, "Analysing India's Threat Spectrum", *The New Indian Express*, 16 Nov 2021, accessed 21 Jun 2025, <https://www.newindianexpress.com/opinions/columns/2021/Nov/16/analysing-indias-threat-spectrum-2383998.html>

⁵ Verma, "Non-Contact Warfare (NCW)".

⁶ IDSA, *Hybrid Warfare*.

⁷ Armin Krishnan, "Fifth Generation Warfare, Hybrid Warfare, and Gray Zone", *Journal of Strategic Security* 15, no. 4 (2022), pp 14–31, accessed 20 Jun 2025, <https://digitalcommons.usf.edu/jss/vol15/iss4/2/>

⁸ Peter Dobias and Kyle Christensen, “The ‘Grey Zone’ and Hybrid Activities”, *Connections: The Quarterly Journal* 21, no. 2 (2022), pp 41–54, accessed 21 Jun 2025, https://procon.bg/system/files/21.2.03_greyzone.pdf

⁹ Hasnain, “Analysing India’s Threat Spectrum”.

¹⁰ “India Cyber Threat Report 2023”, *Data Security Council of India*, New Delhi, 2023, accessed 21 Jun 2025, https://www.dsai.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

¹¹ S Singh, “The Battle Beyond the Frontlines: Social Media Driven Information Warfare in the India-Pakistan Context”, *Centre for Joint Warfare Studies*, Jul 2023, accessed 25 Jun 2025, <https://cenjows.in/the-battle-beyond-the-frontlines-social-media-driven-information-warfare-in-the-india-pakistan-context/>

¹² Rajeswari Pillai Rajagopalan and Dimitrios Stroikos “The Transformation of India’s Space Policy: From Space for Development to the Pursuit of Security and Prestige”, *Space Policy*, Elsevier, 14 May 2024, accessed 15 Aug 2024, <https://www.sciencedirect.com/science/article/pii/S0265964624000249>

¹³ Brigadier Narender Kumar, “Hybrid Warfare Division—An Urgent Operational Requirement for India”, *Journal of the United Service Institution of India*, vol. CL, no. 620 (Apr–Jun 2020), accessed 12 Jun 2025, <https://usiofindia.org/pdf/8—USI%20Journal%20Apr-Jun%202020-74-83.pdf>

¹⁴ Verma, “Non-Contact Warfare (NCW)”.