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

Flight Lieutenant Vatsalya Yadav@

Abstract

This article examines the evolution of warfare, focusing on the emergence and implications of non-contact and non-kinetic conflict in the 21st Century. Tracing the trajectory from classical battlefields to fifth-generation warfare, it underscores how cyber operations, information manipulation, and economic and diplomatic coercion have redefined military strategy. This article particularly explores the Indian context, detailing how hybrid threats—from cyber-attacks to disinformation campaigns—challenge national security. Through case studies such as cyber disruptions in Mumbai and disinformation in Kashmir, it highlights India's vulnerabilities and adaptive responses. It further outlines the capabilities and challenges India faces in cyber warfare, information dominance, and economic resilience. To strengthen national defence, this article recommends integrated strategies across cybersecurity, strategic communication, indigenous technological advancement, and interagency coordination. Ultimately, this article advocates for a multifaceted, future-oriented approach to equip India against the complex realities of non-kinetic and grey-zone warfare.

@**Flight Lieutenant Vatsalya Yadav**, an alumnus of the Air Force Technical College and Air Force Academy, was commissioned into the Technical Branch on 04 Jan 2020. He is currently posted with the Air Force Cyber Group and is a keen cybersecurity enthusiast and researcher.

This is the first prize winning essay in the USI Gold Medal Essay Competition 2024.

Journal of the United Service Institution of India, Vol. CLV, No. 640, April-June 2025.

Introduction

Warfare has undergone significant transformations throughout history, transitioning from the era of swords and shields to mechanised armies, and now into the sophisticated realm of non-contact and non-kinetic strategies. In ancient times, warfare was characterised by direct confrontation, with physical proximity to the enemy often determining the outcome of battles. The Industrial Revolution brought about mechanised warfare, culminating in the mass mobilisation of armies and the introduction of advanced weaponry during the World Wars. The Cold War era witnessed the emergence of nuclear deterrence and the threat of mutually assured destruction, which significantly reduced direct military engagements between major powers.

In the contemporary world, the nature of conflict is increasingly shaped by advancements in technology, leading to the emergence of Non-Contact Warfare (NCW) and Non-Kinetic Warfare (NKW). These new forms of warfare emphasise achieving strategic objectives through indirect means, such as cyber-attacks, disinformation campaigns, economic coercion, and diplomatic manoeuvres. As noted by RAND Corporation's future warfare studies, the geopolitical landscape has shifted towards a multi-dimensional approach to conflict, where information, automation, and precision have become critical components of military strategy.[1]

The evolution towards NCW reflects a broader trend in global security, where adversaries seek to exploit vulnerabilities in digital networks, information systems, and economic structures without resorting to direct military confrontation. For example, hybrid warfare—a blend of conventional and unconventional tactics—has blurred the lines between combatants and civilians, as well as between war and peace. Cognitive warfare, another modern development, targets individuals' cognition and decision-making processes, often using disinformation and psychological operations, to disrupt societal cohesion.[2]

This transformation is particularly relevant for India, a nation positioned at the crossroads of traditional threats and emerging challenges. India faces conventional military threats from neighbouring adversaries such as China and Pakistan, alongside more modern threats in the digital and cognitive realms. Cyber-attacks targeting critical infrastructure, disinformation campaigns aimed at destabilising public opinion, and economic coercion through trade restrictions have all become part of India's security landscape.

Historical Context of Fifth-Generation Warfare (5GW) in India

The historical development of warfare is categorised into generations, each characterised by specific technological advancements, strategic shifts, and operational tactics. Understanding this evolutionary path helps to contextualise India's adaptation to 5GW and its focus on non-contact and non-kinetic operations.

First to Third-Generation Warfare (3GW): The Foundations of Conventional Conflict.

- **First-Generation Warfare**. It refers to the period of classical conflicts where battles were fought with massed manpower, rudimentary weapons, and close-quarter combat. It was an era dominated by direct, physical engagements with infantry, cavalry, and basic artillery. Major historical battles such as those of the Napoleonic Wars exemplify this form of warfare, where strategies revolved around the positioning of large armies on battlefields and the direct clash of forces.

- **Second-Generation Warfare**. It emerged with the Industrial Revolution and marked a shift towards mechanised warfare. This period saw the introduction of mass mobilisation, artillery, machine guns, and trench warfare, as epitomised by World War I. The nature of conflict shifted from hand-to-hand combat to industrialised killing machines, leading to unprecedented levels of destruction. Military strategies became more sophisticated, relying on firepower and the capacity to sustain long battles through logistics and industrial output.

- **Third-Generation Warfare**. Also known as manoeuvre warfare, it emerged during World War II and is perhaps best illustrated by the German strategy of *Blitzkrieg* (an intense military campaign intended to bring about a swift victory). This strategy introduced mobility, speed, and the integration of combined arms (infantry, artillery, and air power) to overwhelm opponents. Rather than focusing on grinding, static engagements, 3GW emphasised surprise, rapid advancements, and encirclement to disorient and incapacitate enemies. It was a significant leap forward in terms of operational effectiveness and coordination.

Fourth-Generation Warfare (4GW): The Rise of Irregular and Asymmetric Conflicts 4GW.

- **Origins and Evolution of 4GW**. It emerged in the latter half of the 20th Century, driven largely by the decolonisation process, the rise of non-state actors, and the proliferation of insurgent movements. This form of warfare emphasised irregular, guerrilla tactics and asymmetric conflicts, where weaker forces used unconventional strategies to challenge superior military powers. The Vietnam War, Soviet Afghan War, and more recently, the War on Terror, are key examples of 4GW.

- **Role of Non-State Actors and Blurred Battle Lines**. In 4GW, non-state actors such as insurgent groups, militias, and terrorist organisations became significant players, often operating outside traditional rules of engagement. These actors utilised tactics such as ambushes, sabotage, and psychological operations to undermine state power. 4GW also blurred the lines between combatants and civilians, challenging conventional military responses and complicating the legal and ethical dimensions of warfare.

- **India's Strategic Response to 4GW Challenges**. For India, 4GW presented new challenges, particularly in regions such as Jammu and Kashmir, the Northeast, and the Naxalite insurgencies. India had to contend with insurgent groups that used guerrilla tactics and received external support from adversarial nations. In response, the Indian military adapted by incorporating counterinsurgency and counter-terrorism strategies, relying on intelligence-driven operations, psychological warfare, and strategic use of paramilitary forces.

5GW: A New Era of Technology-driven Conflict.

- **Defining 5GW**. It represents the latest phase in the evolution of conflict, defined by its reliance on advanced technology, cyber capabilities, Information Warfare (IW), and space-based operations. Unlike previous generations, 5GW is not primarily about direct military confrontation or territorial conquest. Instead, it revolves around battles fought in the cyber domain, through influence operations, and by disrupting an adversary's critical infrastructure

- **Tactics and Technology**. In 5GW, the focus shifts to achieving strategic objectives by targeting the cognitive and informational dimensions of the adversary. This could include cyber-attacks that disrupt communications and power grids, disinformation campaigns that sow discord and confusion, and economic coercion that weakens a nation's resolve without firing a single shot. The growing importance of Artificial Intelligence (AI), autonomous systems, and space technologies has further expanded the scope of 5GW, making it a truly multi-dimensional form of conflict

- **India's Cyber Challenge**. India's adaptation to 5GW has been driven by its recognition of emerging threats, particularly from its regional adversaries. The increasing frequency of cyber-attacks targeting India's critical infrastructure, financial systems, and defence networks has underscored the importance of cyber resilience. The attack on Mumbai's power grid in 2020, suspected to be a state-sponsored cyber operation, is one example of how non-contact strategies are being used to undermine India's security

- **Information Warfare Threats**. In addition to cyber warfare, IW has become a key concern for India. Disinformation campaigns, particularly those related to the Kashmir conflict and broader regional disputes, have been used by adversaries to destabilise internal politics and challenge India's international standing. These campaigns exploit the rapid spread of information on digital platforms, amplifying propaganda and false narratives to influence public opinion and sow divisions within Indian society.

India's Response to Fifth-Generation Warfare

Recognising the threats posed by 5GW, India has gradually shifted its focus towards developing the capabilities necessary to counter these new forms of conflict. This includes investing in cyber defence, IW capabilities, space-based technologies, and autonomous systems. The establishment of a dedicated Cyber Command within the Indian Armed Forces is one step towards consolidating cyber defence efforts, though there is still much work to be done to fully integrate these capabilities across all branches of the military.

India is also increasingly involved in space-based operations, recognising the importance of satellite communications, surveillance, and Anti-Satellite (ASAT) weapons in modern warfare. India's successful ASAT test in 2019 demonstrated its growing capabilities in this domain, underscoring its commitment to defending its assets in space while preparing for potential conflicts that may extend beyond the Earth's surface.

Furthermore, the Indian military has begun to explore the potential of autonomous systems, such as drones and unmanned ground vehicles, for surveillance, reconnaissance, and even direct combat roles. These systems reduce the risk to human soldiers and allow for greater flexibility in operational planning, particularly in non-contact scenarios where physical presence on the battlefield is minimised.

India's strategic planners also recognise the need for a comprehensive approach that includes not only military modernisation but also strengthening societal resilience against non-kinetic threats. This involves collaboration between government agencies, the private sector, and international partners to enhance cyber security, protect critical infrastructure, and counter disinformation.

The Concept of Non-Contact and Non-Kinetic Warfare

At its core, NCW and NKW are designed to achieve strategic objectives without resorting to direct physical confrontation. This new form of warfare reflects the broader evolution of conflict, where influence, disruption, and control have become the dominant strategies rather than brute force and territorial conquest. Unlike traditional kinetic warfare, which relies on physical weapons and troop deployments to incapacitate or destroy the enemy, non-kinetic methods operate in domains that are less visible but increasingly critical, such as cyberspace, information networks, economic systems, and diplomacy.

One of the defining characteristics of NCW and NKW is its reliance on technology and innovation to undermine an adversary's ability to function effectively. The goal is not to defeat the enemy through sheer firepower, but rather to create confusion, disable communication networks, disrupt decision-making processes, and erode public confidence. By targeting critical systems that support military operations, governance, and civilian infrastructure, NKW can bring about significant disruption without any physical engagement.

Cyber Warfare.

- Cyber warfare is one of the most prominent forms of NCW and NKW. It involves the use of digital attacks on information systems to disrupt, damage, or steal critical data from the adversary. In an interconnected world where communications, logistics, and control systems are heavily reliant on digital infrastructure, cyber warfare can be highly effective in paralysing military and civilian capabilities.

- Cyber-attacks can take many forms, from simple disruptions to sophisticated operations that target power grids, financial systems, or military command and control networks. These attacks can be carried out remotely, making attribution difficult and complicating responses. The anonymity of cyber warfare provides a degree of deniability to the aggressor, making it a preferred tool for state and non-state actors alike. A successful cyber-attack can cause operational paralysis, disrupt the economy, and instil fear and uncertainty in the affected population—all without a single shot being fired.[3]

Information Warfare.

- IW is another critical component of non-kinetic operations, focusing on the control and manipulation of information to influence the perceptions, beliefs, and actions of target audience. The advent of social media and the rapid spread of digital communication have provided new avenues for disseminating propaganda, misinformation, and psychological operations designed to shape public opinion and political decision-making.

- This form of warfare targets the cognitive dimension of conflict, seeking to undermine an adversary's will to fight or support a particular cause. It often involves spreading disinformation to create confusion, generate dissent, or destabilise governments. IW can also be used to bolster an aggressor's narrative, gaining the support of neutral or even hostile audiences. For example, false narratives may be crafted to paint the adversary as an aggressor, justify military actions, or erode international support for the opposing side. By controlling the flow of information, a state can weaken the resolve of its adversary without direct military engagement.

Electronic Warfare (EW).

- EW targets the electromagnetic spectrum, which is critical for modern military operations. It involves jamming or disrupting the enemy's communication, radar, and navigation systems, rendering their military assets less effective or even useless. By interfering with signals used for coordination, reconnaissance, and precision targeting, EW can cause confusion and force the enemy to operate with reduced effectiveness.

- EW can be used in conjunction with cyber-attacks to create a broader impact on the battlefield, affecting everything from unmanned drones and aircraft to missile systems and ground troops. By degrading the enemy's ability to communicate or use key technologies, EW creates a significant tactical advantage for the attacker.

Economic Warfare.

- Economic warfare seeks to weaken an adversary by targeting its financial systems, trade routes, and economic stability. This form of warfare involves imposing sanctions, trade restrictions, and financial blockades to cripple the enemy's economy. By restricting access to vital resources, cutting off trade routes, and disrupting financial networks, economic warfare can exhaust an adversary's resources over time, forcing them to make concessions or weakening their ability to maintain a prolonged conflict.

- Economic warfare does not require physical confrontation, but it can have a devastating impact on a nation's economy, civilian population, and military capabilities. The effectiveness of this strategy lies in its ability to create sustained pressure that can lead to economic collapse or political instability. Moreover, economic coercion can be used in concert with diplomatic and military efforts to achieve broader strategic objectives without the need for kinetic operations.

Diplomatic Warfare.

- Diplomatic warfare uses the tools of statecraft to isolate, pressure, or coerce an adversary into submission or compromise. It involves forming alliances, leveraging international organisations, and using diplomatic channels to sway global opinion against the adversary. Diplomatic warfare also includes the strategic use of soft power, such as cultural diplomacy and international aid, to build influence and garner support from other nations.

- Through diplomatic manoeuvrings, a state can achieve its strategic objectives without engaging in direct conflict. By isolating the adversary diplomatically, the aggressor can weaken its legitimacy on the global stage, restrict its access to international support, and limit its ability to manoeuvre diplomatically. Diplomatic warfare can also be used to create coalitions that amplify the pressure on the adversary, making it more difficult for them to sustain their position.

Hybrid and Grey-Zone Operations.

- Hybrid warfare combines conventional military tactics with non-kinetic operations, creating a multidimensional approach that blends traditional force with new methods of conflict. Hybrid operations often involve the use of irregular forces, cyber-attacks, economic pressure, and information manipulation in conjunction with conventional military actions. This blend of tactics allows the aggressor to achieve their goals while avoiding the direct costs and risks of full-scale military conflict.

- Grey-zone operations are a subset of hybrid warfare, occupying the space between peace and open warfare. These operations involve activities that are more aggressive than normal state interactions but fall short of triggering a formal military response. Grey-zone operations often include covert or deniable actions, such as cyber-attacks that are difficult to attribute, or the use of proxy forces to engage in low-intensity conflict.[4]

- The ambiguity created by grey-zone operations allows the aggressor to push the boundaries of conflict without crossing the threshold that would provoke a military retaliation.

This approach exploits the legal and ethical grey areas of international relations, making it difficult for the targeted state to respond effectively. Grey-zone tactics can erode trust in institutions, create internal divisions, and weaken the enemy's ability to coordinate a coherent defence.

Case Studies of Non-Contact and Non-Kinetic Warfare in India

India has been subject to multiple instances of NCW and NKW, particularly in the form of cyber-attacks and IW. One notable example is the series of cyber-attacks attributed to state-sponsored actors from China and Pakistan. These attacks have targeted India's critical infrastructure, defence systems, and financial institutions, aiming to disrupt operations and sow chaos. Few of the case studies are as follows:

- **Cyber-Attacks on India's Critical Infrastructure**. In recent years, India's critical infrastructure has come under attack from foreign adversaries. For instance, in 2020, a large-scale cyber-attack targeted Mumbai's power grid, leading to widespread outages across the city. Though the attack was attributed to Chinese state-sponsored actors, the attribution remained ambiguous, making it difficult for India to respond with traditional military measures. This attack highlighted the vulnerabilities in India's cyber defence mechanisms and underscored the need for improved cybersecurity capabilities.

- **Disinformation Campaigns in Kashmir**. The Kashmir conflict has long been a focal point for disinformation and psychological operations. Various state and non-state actors have employed social media platforms to spread propaganda, incite violence, and manipulate public opinion both within Kashmir and internationally. These campaigns aim to delegitimise India's control over the region and to fuel unrest by disseminating false information.

- **Economic Coercion by China**. China has frequently used economic coercion as a tool of NKW against India. For instance, after the 2020 Galwan Valley clashes, China imposed unofficial trade restrictions on Indian goods and boycotted Indian products. In response, India banned Chinese apps and reduced its economic dependency on Chinese imports, exemplifying the tit-for-tat nature of economic warfare in the non-contact domain.

India’s Current Capabilities and Challenges

India’s capability in NCW and NKW is growing, but several challenges remain. The country has made progress in developing indigenous technologies for EW and unmanned systems, but significant gaps still exist, particularly in the cyber domain.

Cyber Warfare.

- While India has established a Cyber Command to oversee its cyber operations, the pace of development has been slow compared to global standards. India lags behind countries like the United States (US) and China in terms of offensive and defensive cyber capabilities. One of the major challenges is the lack of skilled manpower, particularly in cybersecurity and AI. Although India has a robust information technology industry, this expertise has not yet been fully harnessed for national security purposes.

- The bureaucratic hurdles in decision-making further compound the issue, with the integration of cyber operations across the armed forces being hampered by a lack of coordination between different government agencies. India also faces the challenge of indigenous software and hardware production, as much of its infrastructure relies on foreign technology, creating vulnerabilities to external manipulation.

Information Warfare.

- India has made strides in countering IW particularly in handling insurgencies in Jammu and Kashmir and the Northeast. However, it still faces challenges in effectively countering large-scale disinformation campaigns, particularly those originating from adversaries like Pakistan and China. The rapid spread of misinformation through social media platforms poses a significant challenge for Indian authorities, as it can fuel unrest and undermine the government’s legitimacy.

- India’s IW capabilities are also limited by the absence of coordinated public diplomacy efforts. While the armed forces have experience in psychological operations, the lack of synergy between military and civilian institutions hampers the effectiveness of these operations on a national and international scale.

Economic Warfare. Economic warfare remains an area where India has both strengths and weaknesses. India's growing economic clout provides it with leverage in diplomatic negotiations and trade disputes. However, its reliance on imports for key sectors such as energy and technology makes it vulnerable to economic coercion from larger powers like China. The COVID-19 pandemic further highlighted these vulnerabilities, as disruptions in global supply chains affected India's ability to access critical goods.

Pathways for Integration of Non-Contact and Non-Kinetic Warfare in India

To overcome these challenges and integrate NCW and NKW into its national security strategy, India must focus on several key areas:

- **Enhancing Cybersecurity Capabilities**. India needs to invest heavily in strengthening its cybersecurity capabilities. This includes building a larger and more skilled cybersecurity workforce, developing indigenous software and hardware, and establishing a more robust Cyber Command structure. Collaboration with the private sector and international partners will be essential for developing offensive and defensive capabilities.

- **Developing Strategic Communication and IW**. India must enhance its capabilities in strategic communication and IW. This includes countering disinformation campaigns more effectively, improving public diplomacy, and leveraging new technologies such as AI to influence public perception. Developing a centralised body to oversee IW efforts across civilian and military sectors would be beneficial.

- **Strengthening Economic Resilience**. Reducing economic dependency on imports, particularly in critical sectors like technology and energy, should be a priority for India. Diversifying trade relationships and fostering greater self-reliance in key industries will reduce India's vulnerability to economic coercion.

- **Investing in Advanced Technologies**. India must continue to invest in advanced technologies such as AI, unmanned systems, and robotics. These technologies will play a crucial role in NCW, allowing India to maintain a technological edge over potential adversaries. Collaborating with international partners on research and development projects will be critical to accelerating technological advancements.

- **Improving Interagency Coordination**. A lack of coordination between government agencies has been a persistent problem in India's approach to NCW. Establishing a centralised command structure that integrates cyber, information, and economic warfare efforts would help streamline decision-making and improve the effectiveness of India's operations.

- **Building Alliances and Partnerships**. In an increasingly interconnected world, no country can tackle the challenges of NCW and NKW alone. India should focus on building alliances with like-minded countries to share intelligence, develop new technologies, and collaborate on cyber defence and IW. Partnerships with countries like the US, Japan, and Australia could provide India with valuable insights and access to cutting-edge technologies.[5]

Conclusion

NCW and NKW are reshaping 21st Century conflict. Traditional military tactics, based on direct force, are being supplemented by technology-driven methods in cyberspace, information, and global economics. These new tactics focus on disruption, psychological influence, and deterrence rather than conventional victories.

For India, adapting to this evolving landscape is crucial. Cyber-attacks, disinformation, economic coercion, and grey-zone operations pose significant security challenges, particularly in a region where adversaries use hybrid tactics combining traditional force with cyber and IW.

India must adopt a multi-faceted strategy. Enhancing cyber capabilities is essential due to the growing reliance on digital infrastructure for military, economic, and governance functions. This involves improving both defences and offensive capabilities to deter and respond to attacks.

Investing in IW is also vital. Controlling narratives, countering disinformation, and influencing public opinion are central to modern conflict. India must develop strategic communication tools to project policies and counter misinformation.

Additionally, India should invest in advanced technologies like AI, unmanned systems, and space-based platforms. These innovations are critical for modern military operations, offering enhanced surveillance, precision targeting, and automation. Fostering technological advancement will help modernise India's Armed Forces and maintain a competitive edge.

Improving interagency coordination is equally important. Non-contact threats span cyberspace, information systems, and economy, requiring a unified response. Effective defence necessitates cooperation among military, intelligence, civilian, and private sectors. Developing frameworks for seamless coordination is crucial for addressing hybrid threats.

As NCW and NKW grow in importance, India's defence strategy must focus on cyber resilience, strategic communication, and technological innovation to maintain security and influence in an evolving conflict landscape.

Endnotes

[1] "Non-Contact Warfare: Lessons from the US National Defence Strategy", *Neliti*, 2023, accessed 18 Aug 2024 https://media.neliti.com

[2] "Cognitive War Turns the Mind into Battleground", *IE Insights*, 2023, accessed 21 Aug 2024 https://www.ie.edu

[3] "Assessing the Non-Kinetic Battlespace", *The Heritage Foundation*, 2023, accessed 22 Aug 2024 https://www.heritage.org

[4] "Hybrid Warfare and Non-Linear Combat in the 21st Century," *Global Security Review*, 2023, accessed 24 Aug 2024 https://www.globalsecurityreview.com

[5] "Non-Contact Warfare in the 21st Century", *USI of India*, 2023, accessed 24 Aug 2024 https://www.usiofindia.org

Bibliography

Books

1. Liang, Qiao and Xiangsui, Wang. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

2. Mattsson, Peter A. “Russian Military Thinking – A New Generation of Warfare”. *Journal on Baltic Security*, Volume 1, Issue 1, 2015.

3. Cohen, Raphael S and Robinson, Linda. “Political Warfare is Back with a Vengeance”. *RAND Corporation*, 2018.

Articles

4. Narayanan, Rajiv. “Evolution of Warfare and Technology-1”. *Indian Defence Industries*, 08 Dec 2018.

5. Sankar, R. “War by Other Means: Why India Needs to Embrace Irregular Warfare”. *The Week*, 03 Nov 2018.

6. Kumar, Davinder. “No Contact Warfare and the China Factor”. *Scholar Warrior*, Spring 2014, pp 76-78.

7. Kanwal, Gurmeet. “A Pragmatic Experiment: Defence Planning Committee”. *Deccan Herald*, 11 Oct 2018.

Reports

8. Department of Defense. Sharpening the American Military’s Competitive Edge, Summary of 2018 National Defense Strategy of The United States of America. Washington, DC: Department of Defense, 2018.

9. Committee of Experts under Chairmanship of Justice B.N. Srikrishna. A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. Ministry of Electronics & Information Technology, Government of India, 2017.

10. China’s Military Strategy. The State Council Information Office of the People’s Republic of China, Beijing, May 2015.