USI Monograph No 5 - 2025

Information and Cyber in Non-Kinetic Warfare: Counter Strategies

Lieutenant General DP Pandey, PVSM, UYSM, AVSM, VSM (Retd)

(Estd.1870)

United Service Institution of India (USI)
New Delhi

About the Monograph

This monograph explores the evolving character of global contestations, competitions, and conflicts, which have traditionally been driven by the threat of physical or kinetic destruction. As the world transitions toward a digitally interconnected environment, regimes of denial and disruption—manifesting as non-kinetic warfare—are becoming the preferred strategic tools. This monograph highlights the growing centrality of cyber infrastructure and the information domain, which, due to their global reach and cost-effective scalability, are now key instruments for shaping perceptions, manipulating narratives, and influencing behaviours across populations—be they friendly, adversarial, or neutral. It underscores the urgency for India's strategic community and policymakers to fully comprehend and integrate the dimensions of information and cyber warfare within the broader national security framework. By doing so, India can better prepare for the full spectrum of future conflicts, from peace to war and everything in between.

Information and Cyber in Non-Kinetic Warfare: Counter Strategies

Information and Cyber in Non-Kinetic Warfare: Counter Strategies

Lieutenant General DP Pandey,
PVSM, UYSM, AVSM, VSM (Retd)

Est 1870

United Service Institution of India (USI)
New Delhi

Published by

The United Service Institution of India

Rao Tula Ram Marg,
New Delhi - 110 057
website: www.usiofindia.org

First Published in India in 2025

The views expressed in this book are of the author/authors in his/their personal capacity and do not represent the views of the US

Contents

Introduction

Non-Kinetic Warfare (NKW), often referred to as 'Soft Warfare'[1], involves methods of conflict that do not rely on traditional physical violence, such as bombing or shooting. Instead, it focuses on non-physical means of influence, manipulation, and disruption. The rise of the digital age, with its rapid advancements in information technology and cyber capabilities, have dramatically expanded the scope of NKW. In this monograph, the information and cyber aspects of NKW will be explored, focusing on how they function as tools of modern conflict and contestation, and the counterstrategies that need to be developed to combat these growing threats.

The significance of NKW and the centrality of information and cyber domains are yet to be fully assimilated globally, except by the United States (US), China, and perhaps a few other countries. Its importance is surely understood by the non-state actors and corporations who are ahead in exploiting this facet of warfare to achieve their end state and objectives.

While the varying impact or distinction between kinetic and non-kinetic operations may be debated in an operational environment, the recently paused Operation Sindoor—and the ensuing imbroglio between India and Pakistan beginning on the night of 06-07 May 2025—provides salient lessons on the interplay between kinetic and

NKW. Kinetic capabilities will be used to degrade, deter, and restrict the response actions, while non-kinetic capabilities led by information operations will be simultaneously used to shape opinion and decision cycles of the observe, orient, decide, and act loop.[2]

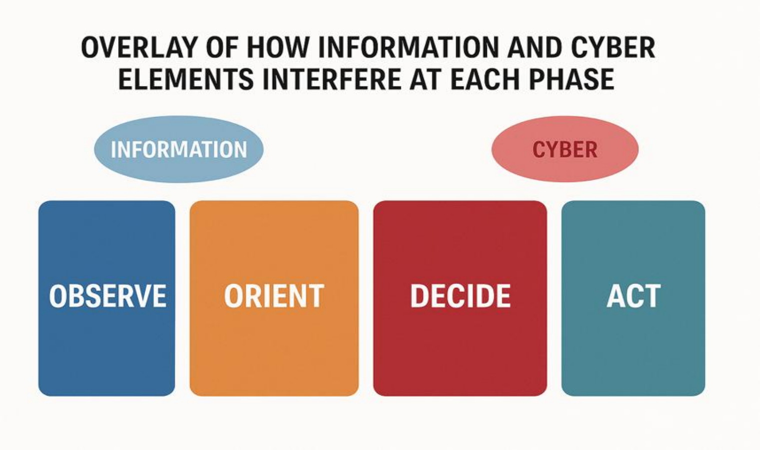

OVERLAY OF HOW INFORMATION AND CYBER ELEMENTS INTERFERE AT EACH PHASE
INFORMATION
CYBER
OBSERVE
ORIENT
DECIDE
ACT

Figure 1: The Observe, Orient, Decide, and Act Loop

While the subject has been lectured, discussed, and beaten to death in the Indian civil-military leadership and policymaker environment, its centrality for a whole-of nation approach is yet to manifest into actionable direction. The import of NKW is yet to be comprehended by the Indian strategic and practitioner community, particularly the uniformed ones, for whom the visible and cognitive deliverables for destruction in terms of kinetic force remains central. The highest form of a battle or war—'Winning without fighting'—remains an incomprehensible concept due to a lack of capacity for lateral and non-linear thinking, compounded by a deep, detailed, and ingrained focus on physical warfighting tactics developed over years and decades among military and security professionals.

The Indian strategic community continues to disregard the stated philosophy on Information Warfare (IW) laid out in simple terms by its own strategic thought leader, Chanakya, who is the ultimate guide on statecraft and the author of *Arthaśāstra* (The Science of Material Gain), a treatise on policy making and military strategy. Chanakya said "An arrow shot by an archer may or may not kill a single person; but skilful intrigue, devised by a wise man, may kill even those who are in the womb". He has also quoted that "If the end could be achieved by non-military methods, even by methods of intrigue, duplicity and fraud, I would not advocate an armed conflict".[3]

On the other hand, the proclaimed and pronounced India's principal enemy, China, has gone by the book *The Art of War*—an influential work on military strategies written by Sun Tzu, the Chinese general, strategist, and philosopher, to adopt the philosophy as its own strategic direction. He states, "The supreme art of war is to subdue the enemy without fighting".[4]

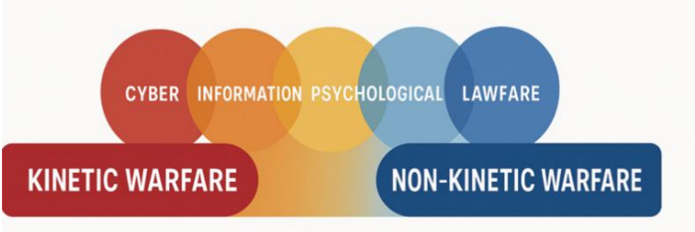


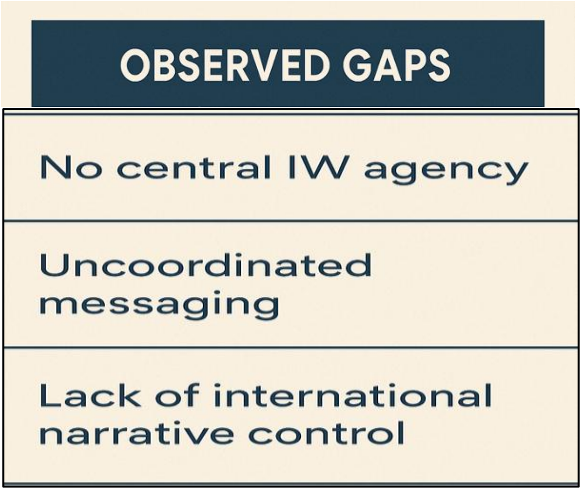
Figure 2: Kinetic to Non-Kinetic Warfare

Chapter 1

Evolving Landscape of Modern Warfare

Operation Sindoor: A Comprehensive Lesson on Centrality of Information and Cyber Warfare in the Non-Kinetic Warfare Domain

Even for the uninitiated in India, the centrality of information and cyber warfare could not have been more evident. While India clearly edged out Pakistan in an 88-hour military engagement, albeit without crossing the Line of Control and International Boundary, an overall perception and belief prevails within the country and the world across that India found itself behind the curve in the information war. The narrative running was absent and a central organisation to manage or lead the information campaign was conspicuously missing. It had to be so, as there is no formal structure or mandated organisation for running information operations. The disparate organisations of the three services and the office of the spokesperson of Ministry of External Affairs (MEA) were operating in an ad hoc manner. While the symbolism of two women officers led by the spokesperson of MEA was greatly appreciated but the plot was lost on the second day as the gravitas following an international and serious event was missing due to the lacklustre operational briefings. A modicum of respect was returned once the Director Generals of Military Operation from the three services conducted the media briefings after four days. The interventions and controlling the narrative at the international level did not even take off. In the end, fractured political voices left the masses and the world community was confused about the rationale and outcome of the entire operation. The entire information campaign was left to be managed by the media houses, with little evidence of operational targeting and the political handles to claim victory based on rhetoric.



OBSERVED GAPS

No central IW agency

Uncoordinated messaging

Lack of international narrative control

Figure 3: Observed Gaps

In the cyber domain, the defence systems were able to withstand attacks led by Pakistan—carried out by its military and various types of hackers and coordinated from multiple countries. However, there were no known, credible, or proven offensive cyber-attacks on Pakistani infrastructure or its allies. It would be reasonable to presume—given the absence of significant outcry from the Pakistani side regarding cyber-attack allegations—that only a modicum of cyber-attacks, if any, were conducted by India.

Sans defined structures, responsibilities, and manning, India will lag in the domains of information and

cyber warfare. Not only are adequate government-owned systems necessary, but it is also imperative to involve private and individual players. A long-term investment is a must if the next campaign, even short of war, is conducted with China, an adversary with technology, immense funding, huge Human Resource (HR) talent, and an authoritarian regime. China as such conducts information and cyber warfare, in peace time investing funds, training workforce, and creating technological solutions for competing with the North Atlantic Treaty Organization (NATO) led by the US. India, based on its doctrine of strategic autonomy, must prepare to not only defend but also take the battle across to China by breaching the iron wall of information and cyber warfare. There is no partnership or alliance that will fight or even remotely be side of India.

Relevance of Information and Cyber Aspects in the Contemporary World

As the entire world is benefitting from the expansion and proliferation of the digital world for ease of living, the radical and extremist elements, as well as some nation-states, seek to exploit the same platform to subdue or control adversaries, competitors, and even allies and their own populations. Therefore, the exploitation of data to manipulate the existing societal eagerness to consume easily available information—

and to control or disrupt cyberspace and networks due to increasing reliance on digital infrastructure—should be a central focus of interest, concern, and action. The growing role of social media in regional and geopolitical affairs, as witnessed in the recent US elections—wherein Donald Trump received support from Elon Musk, the owner of X (formerly Twitter), and the Democrats were reinforced by Mark Zuckerberg, the owner of Facebook—has made this topic especially pressing. Russian interference in the 2016 US election or the 2020 SolarWinds cyber-attack[5] are few other examples that contextualise the importance of information and cyber warfare.

The rise of cyber threats, the increasing reliance on digital infrastructures, and the growing role of social media in geopolitics have made this topic especially pressing. A few lines focusing on the 'Why Now' aspect could enhance the reader's understanding of the position of this subject.

While NKW does not involve direct physical confrontation or the use of kinetic weapons, it is believed commonly that NKW is often used in conjunction with kinetic warfare. Nothing can be further from this misplaced perception. NKW is ongoing during peace, war, post war, as is evidenced in the ongoing narrative battle between India, Pakistan, China, the US, and political parties in all the countries before, after, and during pause of Operation Sindoor, and during entire spectrum in between. It is prosecuted between states, non-states, corporations, businesses, political parties, friends and enemies, allies, and partners, as more often than not the states engage indirectly with fronts and not directly, to avoid confrontation. For example, Elon Musk-owned Starlink communication system powering Ukraine against the Russians in the ongoing conflict of past three years since 24 Feb 2022, avoids the US and the NATO from a direct involvement. Ukraine requested the US aerospace company SpaceX to activate their Starlink satellite internet service in the country, to replace internet and communication networks degraded or destroyed during the war.[6] Similarly, use of the mega social media portals to influence elections in a country to position governments with friendly and pliable postures is a part of NKW.

While NKW threats lie in the realms of cyber warfare, Electronic Warfare (EW), IW, PSY, lawfare, or economic warfare, there are new emerging trends like regimes of technology denial and sanctions, etc. NKW is prosecuted with a view to cause disruption of critical infrastructure, theft, or manipulation of sensitive information, undermining of public trust and confidence, erosion of economic stability, shaping of minds of the target population, and creation of unrest in the target country or population.

Understanding Non-Kinetic Warfare

NKW is a broad and evolving concept. Unlike kinetic warfare, which typically involves direct physical confrontation, NKW uses Psychological Operations (PSYOPS), informational, lawfare, economic, and cyber tools to influence, deceive, disrupt, or incapacitate an adversary's political, economic, and social systems. These methods can range from information operations to cyberattacks, social media manipulation, disinformation campaigns, and PSYOPS.

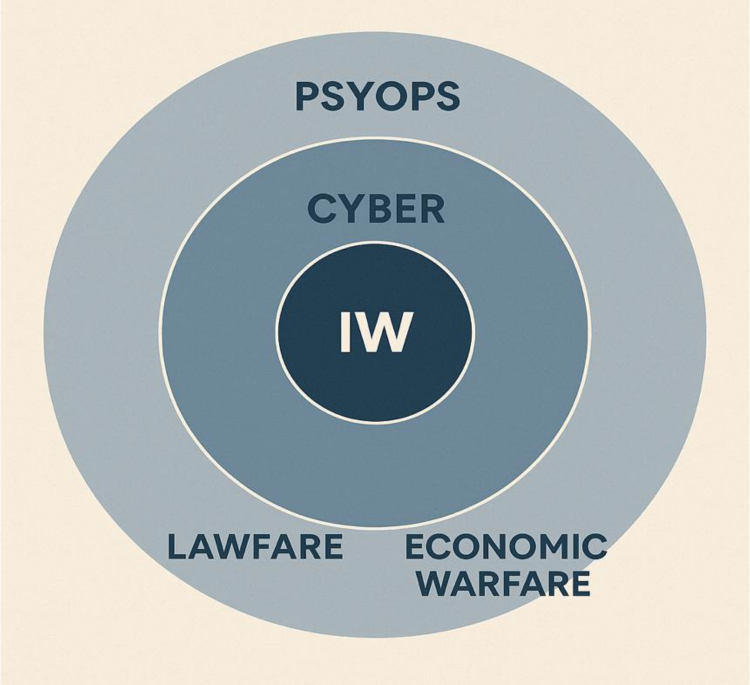


Figure 4: Non-Kinetic Warfare

The advent of the internet, social media, and advanced cyber capabilities has made NKW increasingly potent, allowing state and non-state actors alike to engage in complex, multi-dimensional strategies. These types of operations can be executed with a degree of anonymity, often leaving little trace or clear attribution, making them harder to detect and counter.

Chapter 2

Strategic Disruptions in the Non-Kinetic Realm

Kinetic Consequences of Non-Kinetic Warfare: New Realities

Thousands of explosions struck Hezbollah members on 17 Sept 2024, exploding pagers and walkie-talkies on 18 Sep 2024, which killed at least 37 people—including some children—and injured nearly 3,000, according to Lebanese health authorities.[7] This attack neutralised the entire Hezbollah leadership during the ongoing Israel-Hamas-Hezbollah conflict. The terminology of NKW may have crossed the grey-zone leaning towards the possibility of kinetic warfare application of cyber. In any case, the consequences of the cyber-attacks towards denial of essential services—such as power cuts or disruptions in road or railway signalling systems resulting in deaths or injuries—no longer remain within the realm of NKW. Manipulation of a mob through fake or disinformation campaigns, resulting in lynching or large-scale destruction, also borders on the kinetic application of IW. While out of the scope of this monograph, there is a need to question if NKW, in the domains of information and cyber, is getting weaponised and kinetic.

Enhanced Threat of Non-Kinetic Warfare in Terms of Information and Cyber Aspects

While information was always a part of warfighting in terms acquisition, deception, misinformation, etc., even in ancient times, both prior and during wars, its impact and influence

was restricted in terms of geography and outreach to segments of the target population. What has changed in the contemporary world is the 'Instantaneous Age' phenomena brought by the internet and ever evolving technologies that has ensured flattening of the information world, where the entire world consumes same information simultaneously. Similarly, the reliance of the physical world and the digital space on wires and waves for basics of livelihood and living has ensured the eminence of cyber aspects to affect basic lifestyle. Denial of power or the internet is infringement of human rights in today's world.

As of 2024, there are approximately 4.88 billion smartphone users worldwide, accounting for about 60.42 per cent of the global population. The number of smartphones in use globally is around 7.21 billion. While China leads global smartphone ownership with 974.60 million users, India ranks second with 659 million users.[8] 61.00 per cent of the world population and, of course, 100.00 per cent of military population is on smartphones and connected on at least one form of social media platform. In the developed world, 100.00 per cent of the population is on smartphone or is connected live to some device or other. India accounts for

40.00 per cent of the digital transaction of the world and 80.00 per cent of all digital transactions within the country. 100.00 per cent information, including that on social media and all forms of military and governmental, rides on cyber space because of digital age.

Data Point	Value / Description
Global smartphone users (2024)	4.88 billion
Percentage of global population using smartphones	60.42 per cent
Total number of smartphones in use globally	7.21 billion
Top smartphone user country—China	974.6 million users
Second highest smartphone user country—India	659 million users
Global population on smartphones and social media platforms	61.00 per cent
Military population on smartphones and social media	100.00 per cent
Developed world smartphone/device connectivity	100.00 per cent
India's share in global digital transactions	40.00 per cent
India's share in domestic digital transactions	80.00 per cent

Table 1: Global Digital Penetration

Information and cyber security must be treated as the central pillars of national defence, given the growing interconnectedness of digital infrastructure with every facet of national life. To ensure preparedness in this evolving domain, IW readiness should encompass counter-disinformation tools, enhanced media literacy, and the development of offensive cyber capabilities. A robust, whole-of-nation cyber strategy—integrating public-private partnerships—is essential to safeguard India's digital sovereignty and ensure resilience against increasingly sophisticated threats. As India emerges as a digital giant, its vast digital footprint is both a strategic asset and a potential vulnerability, making its protection an imperative rather than a choice. With the country moving steadily towards a fully digital ecosystem, these vulnerabilities are only set to intensify.

As Cherry Gupta from The Indian Express states, "In the 21st century—an era defined by rapid technological advancements—where dynamic virtual spaces have become an indispensable means of communication and sharing information across the globe, social media has blurred the lines between the virtual and the real world, thereby, transforming the world into a global village, with distance no longer a barrier today". The DataReportal mentions that 5.35 billion or 66.00 per cent of world is on the internet.[9] Furthermore, an analysis from Kepios indicates that the number of active social media users has surpassed 5.00 billion, representing about 62.30 per cent of the world's population. In 2024, India had approximately 821.00 million internet users and 462.00 million active social media accounts, as per Data Reportal and Kepios analysis.[10] The centrality of IW cannot be underscored.

Social media influencers in India, as per various estimates, range from 02.50-03.50 million to 73.00 million[11] and the numbers tied into these influencers can be only left to imagination. On the Indian streets, in metros or remote villages, rich and poor, both are observed to be engaged with some digital device consuming data on a variety of platforms. The vulnerability scope in India can be imagined by the fact that the maximum consumer of social media content includes the digitally vulnerable youth, between 13 and 19 years of age, constituting more than 31.00 per cent population in India or 400.00 million users. With one billion smartphone users in India and 04.90 hours or 31.00 per cent of waking time spent by Indians on smartphones, each one of them is a probable target for information landscape.

Therefore, information gaining, as part of peace and war and everything in between, is the cornerstone of all strategies for states, non-states, corporates, business, and ideologies to get ahead and win. Shaping the mind space has never been easier.

The imperatives for protection of information through disturbance, degradation, and denial cannot be more emphasised in the digital age. It is also important to have hardened infrastructure for defending the systems involved in information collection, information transport, and information protection.[12] In all this, information manipulation is an extremely important facet of IW.

An essential feature of counter-strategy in NKW is public awareness and digital literacy, which may look benign but is essential for the population, including the military. There is also a need to create IW structures premised on centralised control, but decentralised execution harmonised to address the rapid spread of information and the vulnerabilities of cyber infrastructure—especially given its dependence on foreign components in the Indian context. The necessity to create an ecosystem involving public and private organisations and educational institutions cannot be over emphasised. Embracing Artificial Intelligence (AI) and other fast emerging technologies is unavoidable in the flat world where societies and governments have differences on moral and legal issues, but small and big corporations and individuals continue to move on the path of exploiting technology, citing larger good and transparency.

As this form of contestation is new and ever evolving, there is a compulsion to draw adaptive and live doctrines, policies, strategies, and counter-strategies. The whole-of-nation approach is the way forward in the digital age to protect information and critical infrastructure and prevent distortion or manipulation of information.

Direct Linkage between Information Warfare and Cyber Space in Non-Kinetic Warfare

Earlier information took time to travel and to analyse, verify, and exploit. However, with the internet and the ever-increasing capabilities of new technologies, access to information has become significantly easier. With use of AI and quantum computing, its analysis has become all that faster. But on the other side, the use of machines and advanced crypto systems breaking the system codes on which information resides and is transported has become extremely difficult. Possibilities of deception and mind shaping through the cyber space has become central to strategy formulation and implementation. In the 21st Century war-fighting environment, the battle is fought to shape or gain control of minds of all hues of population, friendly and competitive, to win. As in the modern world of digital age, all information rides on the cyber space, hence, there is a very deep connection between the two.

Early Exploitation of Information Warfare through Denial and its Corelation with Technology

On 05 Aug 1914, more than a century ago, the British cut the communication cables of Germany, the first strategic IW act ever involving information and technology. The British had the most advanced undersea telegraph cable network system wrapped around the world for obvious reasons.[13] The British strategists had the dominant position but they wanted to deny the same ability to the Germans. It also provided an intelligence collection and information manipulation opportunity.

Therefore, just before cutting the cables, a man with the job title 'Censor' arrived at the cable station in Porthcurno, Cornwall. On the secluded beach, telegraph cables carrying traffic across the Atlantic came ashore. Similarly, in the office of the Eastern Telegraph Company in the British colony of Hong Kong, another 'Secret Censor' walked into his new office. A similar figure did the same in every far-flung corner of the British Empire, from Malta to Singapore. Once the censors were in position, instructions had told them to send a message to London reading 'Fixity London, Fixed'.

A global system of interception had been instituted. Known as ‘Censorship’, its aim was to prevent intelligence being conveyed to the enemy and to cut off the enemy’s correspondence with his agents. Britain was taking advantage of its dominance of the international telegraph infrastructure to create the first global communications surveillance system, from Cairo to Cape Town, and from Gibraltar to Zanzibar.

50,000 messages would pass through the hands of 180 censors at the United Kingdom (UK) offices alone every single day. Another 400 worked in 120 stations overseas. Overall, 80 million messages would be subject to censorship during the war. The combination of cutting German cables and forcing communications on to British lines provided an intelligence windfall.

Among the messages that Britain intercepted in the World War I was the so-called Zimmermann Telegram, which revealed a German plan to offer the US territory to Mexico and which, in turn, was used to help draw the US to Britain’s side in the war.[14]

Such is the corelation of information and technology. In digital age, it becomes totally interconnected as all information rides on the cyber space. Its control and denial are of paramount importance. And, therefore, the handshake between the ‘Generalists’ and ‘Technocrats’ is an imperative to stay ahead in the domain of NKW.

In this age of specialisation, commercialisation, and competition for the spectrum space, the private players have the fund, technology, reach, and resources. Armed forces and governments on their own are incapable of succeeding against competitors who have synergised their acts as a whole-of-nation approach. A very contemporary example is the help provide by the Elon Musk-owned Starlink communication system to Ukraine. It is virtually a contest of a private corporation allied with a country against another. India is nowhere in such a correlation or synergy.

Chapter 3

Tools and Tactics of Information Influence

The Information Aspect of Non-Kinetic Warfare

Information serves as the primary enabler of influence. Warfare is not merely about the balance of power; it is increasingly focused on the balance of influence. The ability to launch relentless information operations has increased with the digital explosion and cyber penetrative capability of adversaries' systems. The information environment is rapidly evolving, fundamentally challenging the media's role as gatekeepers and agenda-setters. Engineering of influences across identified echo chambers will challenge the government's abilities to control information highways, thereby, exposing people to risk and increasing societal rift.[15]

Gaining of information or its denial is the primary facets of information aspect. Critical information about the competitor or adversary enables gains across the entire spectrum of warfighting or engagements between two stakeholders. As an extension, IW becomes central to both kinetic and NKW. Information is strategically exploited to shape the mind space by influencing perceptions and behaviour—through partial, corrupted, or denied access to critical information—thereby, undermining the opponent's decision-making capabilities. IW includes propaganda, disinformation, and PSYOPS, all designed to manipulate or control the flow of information.

Psychological Operations

Figure 5: Psychological Operations

PSYOPS are another form of NKW. They involve the use of messages and media designed to influence the emotions, motives, and behaviour of individuals or groups. Unlike disinformation, PSYOPS aim to manipulate behaviour or decision-making processes through more direct psychological techniques, which can be tailored to the cultural and social context of the target. For instance, PSYOPS may seek to reduce the morale of the enemy, convince neutral parties to join a conflict, or sway public opinion in a specific direction. In the age of ma communication and 24-hour news cycles, PSYOPS have become more sophisticated, leveraging modern tools like AI and machine learning to predict and influence outcomes in real-time.

Disinformation and Propaganda.

- Disinformation involves the deliberate spreading of false or misleading information with the intent to deceive. Propaganda is similar, but it may also include truthful information selectively presented to influence a target audience's opinions or behaviours. These strategies have long been employed by governments and organisations, but the advent of social media and digital platforms has vastly expanded their reach and impact.
- Social media platforms like Facebook, Twitter, and TikTok can be manipulated to target specific demographics with tailored messages. These platforms allow actors to exploit algorithmic systems to ensure that their narratives reach the widest possible audience, often without being detected. Disinformation campaigns can be particularly effective during times of crisis, when populations may be more susceptible to believing and sharing false information.
- The disinformation campaigns lead to confusion in the target country, at times dividing the political establishment and providing fuel to the opposition parties to elicit responses which compel

the armed forces to either answer or rebut the queries, thereby, providing valuable operational information. The recent Operation Sindoor launched by India and the counter Operation Bunyan Marsoos by Pakistan has set new norms of disinformation campaigns. This is more effective in democracies where militaries are controlled by elected governments and, thus, are prone to public questioning in media and otherwise, even while operations are ongoing. The questioning of the opposition party on number of losses in aircrafts, while military forces were unwilling to divulge any operational information, fed into the disinformation and propaganda campaign launched by Pakistan successfully.[16]

- The non-state actors have mastered and specialised in exploiting the power of internet initially and now the digital space of online platforms for propaganda to radicalise, recruit, and terrorise populations in the target zones, and across the world in general. The Islamic State of Iraq and Syria or Daesh or Islamic State of Iraq and the Levant, and all other such non-state actors have effectively utilised the anonymity of the internet to spread their influence, virtually at no cost.

Social Media Manipulation.

- With the internet and digital space being both affordable and essential in the contemporary world, social media is rapidly replacing legacy media, such as print, television, and even digital platforms managed by major media houses. The perception that each media house is controlled by corporates or individuals with political leanings has led to a trust deficit. This space is now being taken over by social media as the primary medium for information exchange. During the recent standoff between India and Pakistan, social media emerged as the most trusted and widely followed platform for accessing information and sharing breaking news. So much so, breaking all protocols, President Donald Trump took to X (formerly Twitter) to announce ceasefire between India and Pakistan.[17] As the fastest finger first is believed, even if the credibility of the person in question is suspect, the narrative of Donald Trump found resonance even though the daily briefings and the rebutting of the same by India proved that truth was something else. The same was immediately fanned by the Pakistanis, and of course Indian opposition political parties, leaving the disorganised Indian IW system in disarray.

- With a large number of influencers from both sides—and from across the world—sharing information through data, pictures, videos, and expert analyses with common citizens, the outcome of the recent conflict was, in many ways, being shaped and decided on social media platforms. This has led to its manipulation through banning, penetrating, or buying social media influence actively during this recent imbroglio. While the Ukraine-Russia conflict had set the stage for social media manipulation for the past few years, the ongoing situation between India and Pakistan normalised it.

- During the elections in the US and even lately in the UK, the Russians, as claimed by many sources in target countries, used bot networks and troll farms, such as the Internet Research Agency, to shape perceptions of voters. The impact of social media platforms was never so deep.[18]

Fake News and Deepfakes.

- As the power of PSYOPS, more so to target the civilian population of the enemy country, own population, and the world is taking a central role, highly specialised operations to create fake contents in form of videos, news, and paid influencers across the world is the new norm. Trained actors were used to create images and videos—such as scenes of children and civilians dying during drone or air strikes—to attract the attention of human rights organisations and the global community, with the aim of generating outrage over alleged atrocities. This is often amplified by organic influencers with genuine concerns, but more frequently propagated by paid social media and media influencers. Many such images and videos were made by the Ukrainians and Hamas during the ongoing conflicts, wherein the fake news got exposed due to poor quality images or repetition of same actors in different locations. However, by the time this fake news was exposed, the polarisation against Russia or Israel was completed and contest by either side failed to change the overall perception.[19]

- Digitally created fake news is not only a standard practice for the parties involved in the conflict but also for individuals seeking to benefit from it—financially or otherwise. There are numerous reporters, stringers, social media influencers, and opportunists who seek to profit from wars and conflicts without incurring any cost or risk. They create news from the comfort of their homes and sell it through digital platforms to unsuspecting social media consumers. They use images from other conflicts or digitally created visuals to peddle fake news that is picked up and proliferated unwittingly or deliberately by other influencers.[20] AI has now added new dimensions for creating content that is near real life and has contributed significantly in disinformation and misinformation campaigns by targeting the population that is unaware of the feasibilities and power of deepfakes. PSYOPS now have a newer and extremely dangerous tool in the form of AI, which can create deepfakes that remain in the digital space—altering algorithms and perpetuating false narratives indefinitely. Truth has never been closer to being permanently destroyed in the known history of humankind.

Cognitive Warfare

Cognitive warfare is a relatively new concept within the domain of NKW. It focuses on influencing the cognitive processes of individuals and groups—essentially altering how people think, perceive, and react to information. Cognitive warfare can manipulate public opinion, decision-making, and even individual behaviour by exploiting cognitive biases, emotions, and information overload. It is essentially exploitation or leveraging the confirmatory biases for vested causes.

In the information-rich digital age, cognitive warfare can involve the use of 'Fake News', deepfakes, and algorithmic manipulation to target a population's beliefs and attitudes. Deepfakes, in particular, have made it possible to create highly convincing but entirely fabricated videos and audio recordings that can confuse, disorient, or deceive people on a massive scale.

Figure 6: Briefing by Indian Military Authorities

The recent incident at Pahalgam, where tourists were targeted for being Hindus and, thereafter, the limited military strike by India on the terrorist launchpads and their global headquarters in Pakistan-occupied Jammu and Kashmir and Pakistan has been a test case of influencing the decision-making process, not only in India and Pakistan but in various influential countries and the international organisations. The fear of radiation leaks in Kirana Hills[21], where presumably India had dropped missiles, became a rallying point for Pakistan to involve the US that had taken a call to be a bystander with no interest in the emerging scenarios. Thereafter, the pre-emptive and mischievous tweet by President Donald Trump on 10 May 2025, claiming credit for bringing about a ceasefire by offering trade incentives to both sides, became a contentious issue. Pakistan portrayed it as a diplomatic success, asserting that the issue of Jammu and Kashmir had been internationalised and that the ceasefire was brokered on their terms while they held the upper hand. This significantly challenged decision-makers in India, compelling them to respond with facts—diplomatically to the US President and more emphatically to Pakistan. The outrage in the Indian political community, media, and social media, that the Indian Government actions to not exploit staggering success under external influence could have forced the hand to continue with the limited military operations.[22] While this outrage was managed, it greatly dented the muscular image of the present leadership of the country.

Targets of Information Warfare

The aim of offensive IW is to identify a weak spot and to penetrate the adversary's cyberspace by gaining root access to their servers or to compromise a vulnerable computer system, which can lead them to the main computer networks.

The universal targets of IW include critical information storage systems; command, control, communications, computers, intelligence, surveillance, and reconnaissance and logistical systems; decision support and fire control systems; navigation and guidance systems of platforms; social media platforms; public web domains; and other internet of things assets of adversaries.

These IW targets are equally relevant for China, Pakistan, or any other country and non-state actors.

Chapter 4

Doctrines and Strategic Approaches of State Actors

Information Warfare Strategy: China

The Chinese totally believe in Sun Tzu and practice what he preached to the hilt. In *The Art of War*, Sun Tzu clearly defines the centrality of enemy information to identify strength and weakness to achieve strategic advantage while denying own information. These can be extrapolated into larger doctrines and policies. India learnt this to its' simplistic dismay prior, after and during 1962. The Chinese continue to evolve in both dimensions—seeking information and denying it—and, more critically, through deception and mind space management.

The Chinese believe in *Zhixinxiquan* (information dominance) strategy. Their IW strategy is premised on integrated network EW. Rightly so, as it comprises various elements of EW and network-centric warfare techniques. The basic concept of Chinese IW strategy is to deter and disrupt the adversaries' capability to use data by targeting its critical information system and decision-making process, which eventually affects the adversary's will or ability to fight. The other facet is to conduct cyber espionage[23] and PSYOPS.

Five Core Components of Chinese Information Warfare Strategy

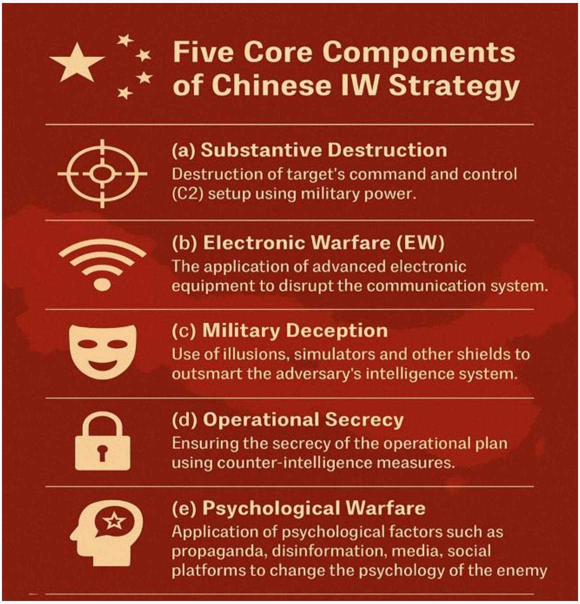
Substantive Destruction. Destruction of targets command and control setup using military power.

Electronic Warfare. The application of advanced electronic equipment to disrupt the communication system.

Military Deception. Use of illusions, simulators, and other shields to outsmart the adversary's intelligence system.

Operational Secrecy. Ensuring the secrecy of the operational plan using counter-intelligence measures.

Psychological Warfare. Application of psychological factors, such as propaganda, disinformation, media, and social platforms to change the psychology of the enemy.



Five Core Components of Chinese IW Strategy

(a) Substantive Destruction
Destruction of target's command and control (C2) setup using military power.

(b) Electronic Warfare (EW)
The application of advanced electronic equipment to disrupt the communication system.

(c) Military Deception
Use of illusions, simulators and other shields to outsmart the adversary's intelligence system.

(d) Operational Secrecy
Ensuring the secrecy of the operational plan using counter-intelligence measures.

(e) Psychological Warfare
Application of psychological factors such as propaganda, disinformation, media, social platforms to change the psychology of the enemy

Figure 7: Core Components of Chinese Information Warfare Strategy

As is seen, the first core component is based on use of kinetic means, second on the cyber domain and balance, while the other three are neither kinetic nor physical but ride on the cyber domains primarily.

China has established control and is monitoring all digital social platforms using *San Zhong Zhanfa* (Three Warfares), a three-pronged strategy, for public opinion/media warfare, psychological warfare, and legal warfare. Initially implemented in Southeast Asia, it is now actively targeted against India. This strategy includes using print and social media, exerting soft power influence through scholarships and investments, influencing opinions within the country, and spreading hate propaganda. Legal warfare is used to 'Bully' border countries to falsely claim a disputed territory as its own and claim territorial rights in adjacent areas through manipulated or conveniently shifting the understanding of land border laws.

The information space management has been best understood and exploited by China, wherein it has contemporary and interesting concepts like TikTok[24] to expand followership and shape the minds; it has used Confucius Institutes[25] in maximum countries to influence the young and senior leaderships. They invest significant funds in media houses[26], political parties, and other influence groups in all countries in the world, particularly the developing ones. While there has been directed effort to influence the world through all platforms, the Chinese have protected their own citizens through a firewall.

Information Warfare Strategy: Pakistan

The Pakistani IW strategy also targets the aforementioned areas; however, its primary efforts focus on PSYOPS, disinformation, and misinformation campaigns against its sworn enemy—efforts that have been conducted both overtly and covertly. It is largely focussed on India through exploiting the fault lines. It has invested heavily in social media accounts, information technology cells, bots, and in its film and television industry. Agile and offensive, it has also invested directly or indirectly to target the information space in India and the world, highlighting the minority rights, human right violations in Jammu and Kashmir and elsewhere, military crisis, political leadership, and alleged Indian involvement in internal affairs of Pakistan. Their Inter-Services Public Relations has a well-oiled machinery and structure for the IW campaigns.

Both Chinese and Pakistanis invest heavily in hiring committed individuals and agencies who operate like paramilitaries, officially and unofficially sanctioned, for offensive actions—in the information domain to target the mind, space, and propaganda and in cyber domain for attacking the infrastructure. A cheap and practical investment with credible deniability.

The IW campaigns are now becoming coordinated with multiple countries joining hands with non-state actors to put India in the spot, particularly during critical periods such as elections or passing of important bills, etc. They also coordinate at different levels to compel India to deviate from its strategic autonomy, posturing to lean towards the West or away from the Russians or to simply control the trade outcomes in their favour. The recent incidents involving the calibrated release of documents by Hindenburg Research LLC—a US investment research firm focused on activist short-selling and reportedly linked to the ill-famed short seller Soros—just prior to critical elections, followed by coordinated attacks across a wide range of social media platforms and legacy media, serve as a warning to the Indian strategic community. Extensively prepared toolkits were used to influence outcomes against the incumbent government in India, which is a clear example of employment of non-state actors by the deep state in the US.

In another example of IW through non-state actors, Stoke White, a UK-based firm, released a 41 pages report titled 'India's War Crimes in Kashmir: Violence, Dissent, and the War on Terror', dated 14 Jan 2022.[27] The report claimed to have gathered testimonies of 2,000 residents of Jammu and Kashmir, primarily Kashmiri Muslims, and alleges that the Indian state puts them under coercion time and again. The report has termed the United Nations (UN)-listed terror groups like Jaish-e-Mohammad and others like the US and the European Union-sanctioned Hizb-ul-Mujahideen as 'Non-state armed groups' and calls for the UK's universal jurisdiction on 'War crimes under the Geneva convention' to be invoked against Indian officials and Indian government functionaries. The theme of the report aligns with Pakistan's long-standing narrative. Even the terms in use are akin to a 2021 dossier, released by Pakistan, titled 'Indian Human

Rights Violations in Indian Illegally Occupied Jammu and Kashmir'.

Stoke White has a link with Turkey, which has colluded with Pakistan in recent years and has been aggressively running a disinformation campaign against India. The two countries, with the assistance of their world-over network, roll out reports and documentaries containing fake information on a sustained regular basis.

Chapter 5

Information Warfare and the Future Operating Environment

Power of Emerging Trends in Information Domain

Apart from the impact of technology itself, the range and depth of influence through the new generation natural language learning processes, such as ChatGPT and even cheaper version DeepSeek, is yet to be appreciated. These are being embedded in almost all domains of society including media, education, finance, and military. The basic flaw which remains is the data from which these models are being trained and the type of stimuli being given to the AI. The quality and especially the content of the data and base models can be very easily manipulated by controlling the information or manipulating it which will have a direct effect on the results and outputs by the users.

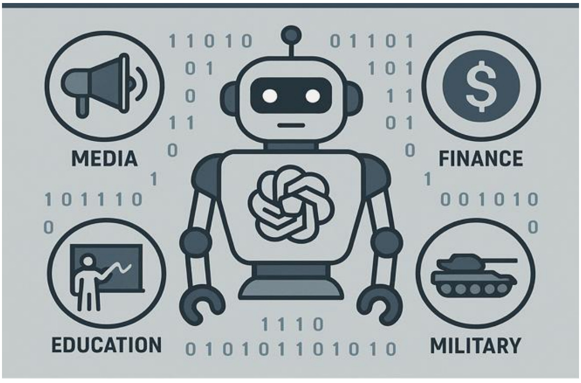


Figure 8: Influence on Domains of Society

With the combination of bots to generate and spread information—whether accurate or not—and the use of language learning models or natural language processing,

countries and non-state actors can manipulate and generate information, rapidly disseminating it across digital platforms worldwide and altering the narrative across the entire information spectrum. Such new age processes in the hands of dictatorial regimes can shape and manipulate the minds of their captive population. With the large corporations controlling the social media platforms or the non-state actors, these cheaper versions can be dangerously exploited. Developed at a fraction of the cost of other AI models—around USD 6.00 mn—DeepSeek is not only innovative but also highly cost-effective. It is free to use, making it accessible to many users. Its affordability and accessibility have contributed to its rapid rise in popularity, earning it the title of the most downloaded app on the AppStore as of 27 Jan 2025.[28] It is likely to give a competition to ChatGPT launched in Nov 2022. The attempts by number of media and others to elicit a response regarding the Tiananmen Square incident and Indias' control on Arunachal Pradesh drew a blank from DeepSeek, as a clear indicator of times to come in the IW when a larger number of users across the world would start exploiting this free version.[29]

Chapter 6

Cyber Threats and Offensive Capabilities

The Cyber Aspect of Non-Kinetic Warfare

Cyber warfare, another pillar of NKW, refers to the use of digital technologies to disrupt, damage, or infiltrate an adversary's systems, infrastructure, or networks. Cyberattacks can be highly destructive and often achieve strategic objectives without causing physical harm. These operations have the potential to disrupt communication systems, power grids, financial institutions, and military operations.

With the advent of more advanced tactics like Advanced Persistent Threats (APTs), supply chain attacks, or the use of AI-driven cyber-attacks, which are becoming more common, the threat to the cyber grids have become much challenging. Stuxnet (used against Iran's nuclear program), Cozy Bear (APT29), Deep Panda (known for hacking Adobe), Fancy Bear (APT28), OilRig, and Helix Kitten (linked to Iranian cybercrime targeting financial and telecommunications sectors) are a few recent examples of APTs.[30]

Space has emerged as an important and worldwide preferred domain along which the communication system is likely to reside. With possibilities of ocean bed lines being prone to disruption, space is the future for communication, providing a high degree of reliability and stability with cost effectiveness. Space systems, including satellites, are vulnerable to cyberattacks, such as data manipulation, signal interference, and Denial of Service (DoS) attacks.

Even this domain now is becoming a heavily contested zone with nations racing to have their presence in space to ensure multitudes of options. The emergence of private sector like SpaceX has now allowed even non-state actors or smaller corporates to have access or control space for leverage of cyber space.

The rise of AI and machine learning in cyber operations will power the threat actors to the new and evolving cutting-edge technologies to breach the cyber defences through far more sophisticated attacks without attribution.

Cyber Espionage

Cyber espionage involves the use of digital tools to infiltrate an adversary's systems to steal sensitive information. Governments and organisations engaged in cyber espionage often seek to gain intelligence on economic, political, or military affairs. Data breaches and hacking of private or government systems can lead to devastating losses, as seen in high-profile cases like the 2017 WannaCry ransomware attack[31] or the 2020 SolarWinds hack. ZhenHue Data leaks of Sep 2020 was a typical case wherein data of at least 800 New Zealanders—politicians, judges, business leaders, journalists, and even criminals—were collected by the China-based company, which has been linked to Chinese military and intelligence.[32] These cases are not only military-linked but can be exploited for IW by a range of agencies starting from blackmail, compliance, or even identifying motivations and orientations of high profile leaders of a country.

In NKW, cyber espionage is a highly effective means of gaining strategic advantages. It allows adversaries to steal critical intellectual property, proprietary technologies, or classified information, all without direct confrontation.

Denial of Service and Distributed Denial of Service (DDoS) Attacks

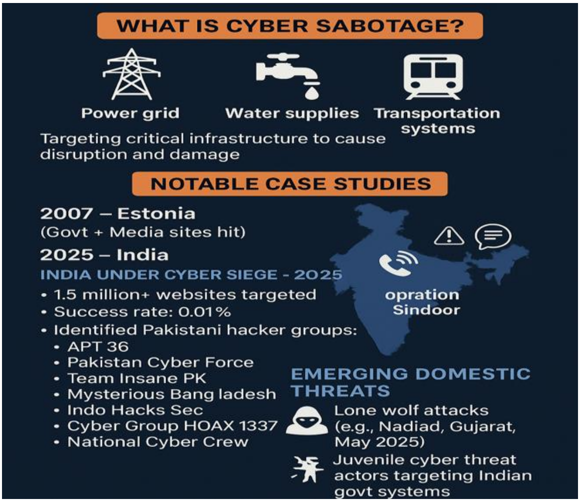
DoS and DDoS attacks are tactics designed to overwhelm and disrupt an opponent's digital infrastructure.[33] These attacks involve flooding a system with an overwhelming amount of traffic, causing it to crash and become unavailable to users. DDoS attacks are particularly common because they are relatively easy to execute and can disrupt the services of governments, businesses, or military organisations.

In the context of NKW, DDoS attacks can be used to cause economic disruption, create chaos, and reduce trust in critical infrastructure, especially when public services such as banking or healthcare are targeted.

Cyber Sabotage and Hacking

Cyber sabotage involves the deliberate targeting of critical infrastructure to cause damage or disruption. In NKW, cyber-attacks on infrastructure such as power grids, water supplies, or transportation systems can have far-reaching consequences. In 2007, for example, cyber-attacks against

Estonia targeted government websites, financial institutions, and media outlets, resulting in widespread disruption.



WHAT IS CYBER SABOTAGE?

Power grid

Water supplies

Transportation systems

Targeting critical infrastructure to cause disruption and damage

NOTABLE CASE STUDIES

2007 – Estonia
(Govt + Media sites hit)

2025 – India

INDIA UNDER CYBER SIEGE - 2025

- 1.5 million+ websites targeted
- Success rate: 0.01%
- Identified Pakistani hacker groups:
  - APT 36
  - Pakistan Cyber Force
  - Team Insane PK
  - Mysterious Bang ladesh
  - Indo Hacks Sec
  - Cyber Group HOAX 1337
  - National Cyber Crew

opration Sindoor

EMERGING DOMESTIC THREATS

Lone wolf attacks (e.g., Nadiad, Gujarat, May 2025)

Juvenile cyber threat actors targeting Indian govt systems

Figure 9: Cyber Sabotage

Similarly, hacking campaigns, such as the use of malware or ransomware, can be used to infiltrate networks, steal data, or disrupt operations. State and non-state actors alike use cyber sabotage as a means of exerting pressure on adversaries, signalling their capabilities, or creating strategic advantage.

During the recent military operation under Operation Sindoor, launched on 07 May 2025, India was targeted both in an organised manner and by individual hackers. As per media claims, 1.50 million plus Indian websites were targeted by the Pakistani hackers. Seven prominent Pakistani hacker groups were identified in due course. These groups, namely

APT 36, Pakistan Cyber Force, Team Insane PK, Mysterious Bangladesh, Indo Hacks Sec, Cyber Group HOAX 1337, and National Cyber Crew (Pakistan Allied), collectively attacked the Indian infrastructure. While only 150 attacks could succeed, making for an abysmal 0.01 per cent success rate, the sheer numbers and scale must be taken into consideration.[34]

While the enemy countries will conduct cyber-attacks, India needs to be vigilant of domestic coordinated and lone-wolf threats[35] emanating from within the country. The recent case, amongst many, is of an 18-year-old Jasim Shahnawaz Ansari from Nadiad, Gujarat, who was arrested by the Gujarat Anti-Terrorism Squad. He had, along with other juvenile accomplices, launched multiple attacks on Indian Government websites. For each such attack, many attempts go unnoticed and undetected.

Chapter 7

Building a Resilient and Adaptive Response Framework

Counter Strategies for Non-Kinetic Warfare

The rise of NKW has prompted governments, businesses, and individuals to develop counter strategies to defend against the evolving threat landscape. Given the largely invisible nature of these tactics, countering NKW requires a multi-faceted approach.

Blending of Information and Cyber Warfare and the International Linkages

There are many facets of NKW but the blending of IW and cyber warfare in the modern world mandates an all-inclusive line of operation. Cyber operations are conducted to target the information domain for data collection, disinformation, and deception campaigns. Similarly, protection of own cyber networks is an imperative to avoid intelligence losses that can be used for conducting PSYOPS. As NKW is a part of grey-zone warfare conducted even during peace and war and entire spectrum in between, it is important that comprehensive strategies be outlined and put in effect. During the recent Operation Sindoor launched by India, the preparation prior to launching even the first attack, the period between the Pahalgam terror attack on 22 Apr 2025 and 06 May 2025, the IW campaign by both sides was in full play. In fact, other countries and non-state actors were also involved in a comprehensive IW onslaught, wherein

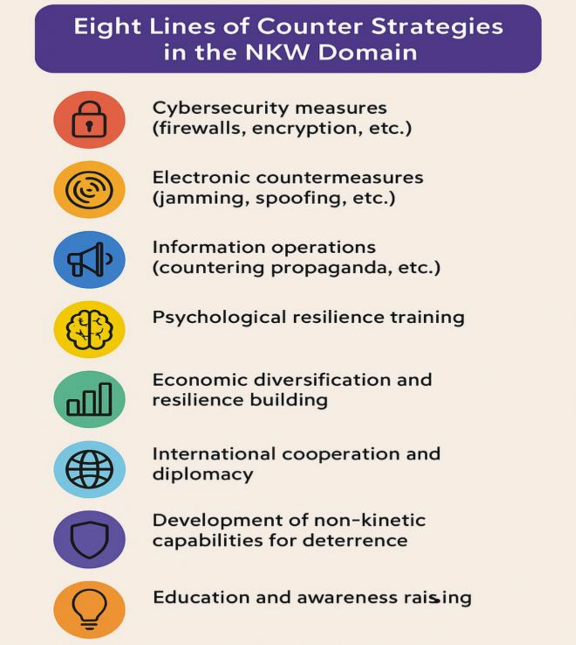
narrative-shaping campaigns were coordinated globally through direct and indirect alliances involving embedded Pakistanis and their supporters in international media. These efforts included trolling, the spread of fake news across both legacy and digital media platforms, and intense activity on the dark web targeting Indian systems through directed cyber-attacks. India stood clearly isolated yet remained resilient and responsive.

Comprehensive Whole-of-Nation Approach Towards Non-Kinetic Warfare

As India remains to adopt a defensive route to IW based on high moral ground and ethical conduct in the international relations, the challenges are multi-fold. However, there continues to be a need for a comprehensive whole-of-nation approach to be a credible non-kinetic force to at least counter these threats, if not prosecute offensive information and cyber warfare, and prepare for new emerging trends in non-kinetic domain. The lines of counter-strategies in NKW domain, therefore, should be eight-fold:

- Firstly, cybersecurity measures (firewalls, encryption, etc.).
- Secondly, wlectronic countermeasures (jamming, spoofing, etc.).

- Thirdly, information operations (countering propaganda, etc.).
- Fourthly, psychological resilience training.
- Fifthly, economic diversification and resilience building.
- Sixthly, international cooperation and diplomacy.
- Seventhly, development of non-kinetic capabilities for deterrence.
- Eighthly, education and awareness raising.



Eight Lines of Counter Strategies in the NKW Domain

Cybersecurity measures (firewalls, encryption, etc.)

Electronic countermeasures (jamming, spoofing, etc.)

Information operations (countering propaganda, etc.)

Psychological resilience training

Economic diversification and resilience building

International cooperation and diplomacy

Development of non-kinetic capabilities for deterrence

Education and awareness raising

Figure 10: Counter Strategies in Non-Kinetic Warfare Domain

Counter-strategy for IW and cyber operations in NKW should be premised on two pillars. The first is technological; based on strengthening the technical infrastructure to defend against cyber-attacks and misinformation campaigns. Secondly, through information and education, wherein public awareness and education needs to be ramped up through campaigns and initiatives to increase cyber literacy among the general public and officials.

Information and Cyber Defence and Resilience

Building robust cybersecurity systems is a critical countermeasure against cyber-attacks. Governments and organisations must invest in securing their networks, software, and data from hackers and malicious actors. This includes adopting advanced threat detection technologies, conducting regular penetration testing, and fostering strong information-sharing networks between public and private sectors.

Moreover, improving cyber resilience—by creating systems that can quickly recover from attacks—can help mitigate the impact of cyber warfare. Ensuring backup systems and data redundancy are in place allows for quicker recovery from cyber disruptions.

Protection of Information through Information Disturbance, Degradation, and Denial. The important facets of IW are disturbance, degradation, and denial. All three techniques are means to the same general end—

preventing the enemy from getting complete, correct information. Because of their similarity, many of the same platforms are used to achieve one or more of the goals. As such, it makes sense to discuss them together. Some of the more commonly used tools in IW include spoofing, noise introduction, jamming, and overloading. Protecting information requires robust infrastructure and secure systems. There are systems on which information rides and strengthening of these will protect information.[36]

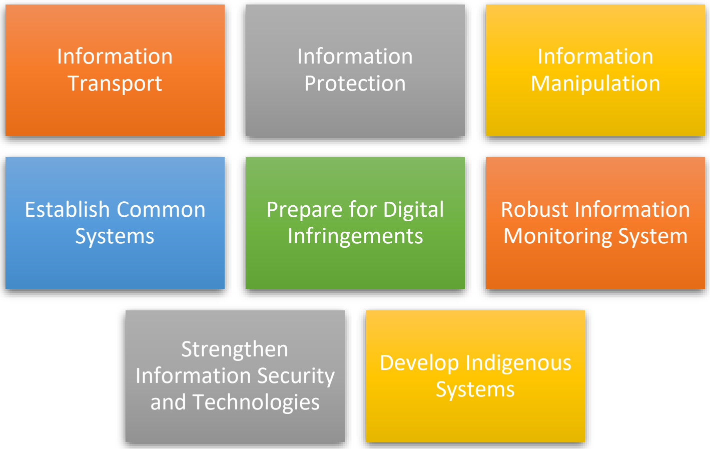

Information Transport
Information Protection
Information Manipulation
Establish Common Systems
Prepare for Digital Infringements
Robust Information Monitoring System
Strengthen Information Security and Technologies
Develop Indigenous Systems

Figure 11: Pillars of National Information Warfare Strategy

Information Collection. India needs to have systems for encryption, spoofing, noise introduction, jamming, and overloading to prevent the enemy's information collection. It will protect the country against information collection attacks and disallow enemy from accessing information.[37]

Information Transport. This is dependent upon infrastructure, and, therefore, the most effective countermeasure for preventing transport is the destruction[38] of the enemy's infrastructure and protecting one's own. It is

important to hide, disguise and prevent destruction or incapacitation of the infrastructure transporting information. If the architecture of information transport is through wire, then the nodes are easily identifiable. They need to be protected.

Information Protection. To counteract enemy efforts to safeguard their information systems, India must develop the capability to protect its own, and penetrate and bypass enemy's protective mechanisms.

Information Manipulation. In the context of IW, this is the alteration of information with intent to distort the opponent's picture of reality. This can be done using several technologies, including computer software for editing text, graphics, video, audio, and other information transport forms.[39]

Establish Common Systems. Common cyber doctrine, procedures, and protocols are important. Training and trade structures for fielding, managing, and auditing the networks is important. Standardisation of equipment and equipment testing agency is important. The second, and perhaps more crucial, key in defending against data manipulation is to prevent the altered data from being re-introduced into the flow of real information. Fortunately, there are several techniques for doing this, the most common of which is redundancy.

Prepare for Digital Infringements. Digital infrastructure will always be prone to infringements by multiple entities, ranging from lone wolves to nation-states. It is essential to prepare for responses to both, in terms of infrastructure disruptions and information manipulation.

Robust Information Monitoring System. It is essential to enhance information security through a strong security framework and a comprehensive monitoring system to track disinformation circulating on social media platforms. Investment in innovation and creativity will continue to drive technology to higher levels of excellence, impacting all aspects of human life—from the way individuals think to the way they wage war and ensure their security.

Strengthen Information Security and Technologies. India must strengthen its existing information security and cryptography technologies and should develop a firewall—like China's Great Firewall—to counter incoming cyber-attacks, disinformation campaigns, and other cyber information operations.

Develop Indigenous Systems. India should take proactive measures to indigenously develop software and other hardware components for defence and security establishment.

Benign and Passive Counter Information Warfare Strategies

Public Information and Digital Literacy. The government has undertaken programmes such as *Satyamav Jayate* (Truth alone triumphs), Pradhan Mantri Gramin Digital Saksharta Abhiyan, and National Digital Literacy Mission to counter disinformation and increase digital literacy. There is also a WhatsApp chatbot and a fact-checking unit under the Press Information Bureau.

Winning the Narrative War. These initiatives are benign and passive, yet necessary. Countering anti-India narratives may be effective only in the short term. However, to win the 'War of narratives', a multi-level set of initiatives and coordinated efforts is required as part of a whole-of-government approach. This must involve all ministries, relevant stakeholders, and even educational institutions to effectively contest IW that seeks to generate discontent and discord. More importantly, offense is the best defence in all forms of warfare, particularly in information and cyber.

Legislation and International Cooperation.

- To combat the growing threat of NKW, governments must implement and enforce legal frameworks that can hold perpetrators accountable. This may involve establishing clear guidelines for cybersecurity, IW, and cyber espionage. Furthermore, international cooperation is crucial to address cross-border challenges posed by cyber-attacks and disinformation campaigns.
- Multilateral organisations such as the UN and the NATO are already exploring ways to develop

international norms and agreements to regulate the use of NKW tactics, particularly in cyberspace. These frameworks can create accountability, deterring rogue actors, fronting nations or corporates, from engaging in such activities.

- Attribution in both information manipulation and targeting of cyber infrastructure will be a challenge. To address this, governments and international organisations must invest in technologies and methodologies for attribution, including the use of digital forensics, AI, and blockchain technologies. Developing the capability to attribute attacks in real-time can help build a more effective deterrence strategy and prevent the escalation of conflict. Therefore, there is also a requirement of investing in judicial processes internationally and nationally.

Importance of Structures.

- Unified structure for centralised control and policy dissemination but decentralised operations and execution is imperative. The Ministry of Electronics and Information Technology (MeitY) plays a crucial role in India's cybersecurity framework. While it is not a direct military or intelligence agency, MeitY is responsible for policymaking, cybersecurity initiatives, and digital infrastructure protection. India has recently released its first joint doctrine for cyberspace operations, acknowledging the importance of cyberspace in modern warfare. Additionally, MeitY has been involved in cybersecurity research, AI-driven security measures, and ethical considerations related to cyber warfare. For direct cyber warfare capabilities, agencies like the National Critical Information Infrastructure Protection Centre and the Indian Computer Emergency Response Team (CERT-In) work alongside MeitY to monitor, prevent, and respond to cyber threats. These are all defensive measures. Space and cyber space are new sovereign domains, and the government business rules must clearly assign responsibilities for its defence.

- At least within the armed forces, the synergy is essential. National Technical Research Organisation, Intelligence Bureau, CERT-In, Defence Cyber Agency (erstwhile Defence Information Assurance and Research Agency), Army Cyber Group, Airforce Cyber Directorate, Naval Cyber Cell, Military Intelligence Directorate, etc., work in cyber security and cyber deterrence. Creation of Command Cyber Operations and Support Wings at Command levels to improve the security of communication networks and increase preparedness in the cyber domain is a step in the right direction.
- An integrated approach is essential, particularly in the Indian context, involving civilian support to prevent and neutralise threats, protect cyberspace, and design a robust information security framework. This is critical for maintaining a secure

digital environment and deterring information-related threats and challenges emanating from adversaries.

Volunteers and Private Networks. India must start believing in the volunteer concept and engage private networks to not only defend the information systems but also take the battle across to the enemy as an offensive manoeuvre. Attack is best form of defence, wherein energy and talent pool of large number of patriotic youths, individually, and in coordinated groups can assist the government agencies that are constrained due to funds, resources, HR, talent pool, introducing emerging and latest technology and legal issues. In Ukraine, the 'Cyber Troops' are essentially volunteers engaged in the collection, collation, and analysis of information from the digital space. They effectively countered sophisticated Russian troll campaigns. Similar to practices in the western world, the engagement of private companies to achieve a multiplier effect in the information and cyber domains warrants serious consideration.

Studies on Operation Sindoor, particularly with reference to India's response in the NKW domain, will take time. However, it is evident that there is significant scope for evolving formal structures and processes to counter the unfair and devious tactics employed in the information and cyber domains. In these areas, culturally self-imposed ethical and moral restraints tend to hinder a whole-of-nation effort, thereby, denying the country any credible strategic advantage.

Conclusion

NKW, particularly in the realms of information and cyber warfare, has become a prominent feature of modern conflict. As technology continues to advance, the potential for non-kinetic tactics to disrupt, manipulate, and destabilise societies grows ever greater. In response, governments, organisations, and individuals must develop robust counter-strategies to defend against these threats, including improving cybersecurity, fostering international cooperation, and promoting information literacy.

While NKW is challenging to confront, a proactive and coordinated approach to both defence and deterrence can reduce its effectiveness and ensure that India remains prepared for this new era of conflict. Understanding and addressing the complexities of NKW is crucial to maintaining national security and safeguarding the integrity of democratic institutions in an increasingly interconnected world.

Massing of effects and balance of influence will continue to be the operating theme for future operations. Penetrative capabilities, persistent presence, and building leverages across the non-traditional security arena will be important. A whole-of-government approach is a must to navigate the complexities of modern-day conflicts. War, if any, may require an even more nuanced approach with across the spectrum exploitation of information and cyber warfare.

Endnotes

[1] Michael L Gross and Tamar Meisels, *The Soft War: The Ethics of Unarmed Conflict,* (Cambridge: Cambridge University Press, 2017), https://www.cambridge.org/core/books/abs/soft-war/introduction/9B576FB6F3B51A4326D6D1530303216F

[2] Brigadier V Verma, *Non-Contact Warfare: An Appraisal of China's Military Capabilities,* (New Delhi: USI of India and Pentagon Press LLP, 2021)

[3] Deepa Jaydev, 'Strategies of Warfare: Chanakya vs Sun Tzu', *International Journal of Creative Research Thoughts (IJCRT)* 6, No. 1 (Mar 2018): 425, accessed 02 May 2025 https://www.ijcrt.org/papers/IJCRT1872227.pdf

[4] Ibid.

[5] Saheed Oladimeji and Sean Michael Kerner, 'SolarWinds Hack Explained: Everything You Need to Know', *TechTarget*, 03 Nov 2023, accessed 05 May 2025 https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[6] 'How Is Starlink Ukraine's Strategic Tool in the Face of Russian Invasion', *The Economic Times,* 15 Feb 2024, accessed 10 May 2025 https://economictimes.indiatimes.com/news/defence/how-is-starlink-ukraines-strategic-tool-in-the-face-of-russian-invasion/articleshow/107710900.cms

[7] Tamara Qiblawi et al., 'Israel Concealed Explosives Inside Batteries of Pagers Sold to Hezbollah, Lebanese Officials Say', *CNN*, 27 Sep 2024, accessed 08 May 2025 https://edition.cnn.com/2024/09/27/middleeast/israel-pager-attack-hezbollah-lebanon-invs-intl/index.html

[8] Sunil Gill, ‘How Many People Own Smartphones in the World? (2024–2029)’, *Priori Data*, last modified 01 Jan 2025, accessed 05 May 2025 https://prioridata.com/data/smartphone-stats/

[9] Cherry Gupta, ‘Top 10 Most Popular Social Media Platforms in 2024: Telegram Ranks 8th Amid Ban Concerns’, *The Indian Express*, 28 Aug 2024, accessed 04 May 2025 https://indianexpress.com/article/trending/top-10-listing/top-10-most-popular-social-media-platforms-as-of-2024-9526794/

[10] Ibid.

[11] Team Kofluence, ‘The Rise of Social Media Influencers in India: Who’s Leading in 2024’, *Kofluence*, 12 Jun 2024, accessed 05 May 2025 https://www.kofluence.com/rise-of-social-media-influencers-in-india/

[12] Mithun Sarkar, ‘Information Warfare: Manipulation of Information in a War’, *Unrevealed Files*, 29 Mar 2022, accessed 05 May 2025 https://unrevealedfiles.com

[13] Gordon Corera, ‘How Britain Pioneered Cable Cutting in World War One’, *BBC News*, 15 Dec 2017, accessed 05 May 2025 https://www.fbcoverup.com/docs/library/2017-12-15-How-Britain-pioneered-cable-cutting-in-World-War-One-by-Gordon-Corera-BBC-News-Dec-15-2017.pdf

[14] Ibid.

[15] V Verma, *Non-Contact Warfare*

[16] Preetha Nair, ‘Rahul Gandhi Steps Up Attack on EAM Jaishankar, Questions Aircraft Losses after Alleged Tip-Off to Pakistan’, *The New Indian Express*, 19 May 2025, accessed 06 May 2025 https://www.newindianexpress.com/nation/2025/May/19/rahul-gandhi-steps-up-attack-on-eam-jaishankar-questions-aircraft-losses-after-alleged-tip-off-to-pakistan

[17] Anirban Bhaumik, ‘Trump Wants to Live Up to Dealmaker Fame with India-Pak Ceasefire’, *Deccan Herald*, 10 May 2025, accessed 15

May 2025 https://www.deccanherald.com/world/trump-wants-to-live-up-to-dealmaker-fame-with-india-pak-ceasefire-3534572

[18] Simon Ostrovsky and Yegor Troyanovsky, 'How Russia Is Using Artificial Intelligence to Interfere in Elections', *PBS NewsHour*, 04 Sep 2024, accessed 12 May 2025 https://www.pbs.org/newshour/show/how-russia-is-using-artificial-intelligence-to-interfere-in-elections

[19] David Klepper, 'Fake Babies, Real Horror: Deepfakes from the Gaza War Increase Fears about AI's Power to Mislead', *AP News*, 28 Nov 2023, accessed 03 May 2025 https://apnews.com/article/artificial-intelligence-hamas-israel-misinformation-ai-gaza-a1bb303b637ffbbb9cbc3aa1e000db47

[20] Rhiannon Stevens, 'A Photographer Created 'Fake' Images of Russia with Generative AI. Now He's Losing His Biggest Fans', *ABC News (Australia)*, 25 Dec 2024, accessed 10 May 2025 https://www.abc.net.au/news/2024-12-26/ai-generated-images-photography-trust/104721106

[21] 'All about Kirana Hills which India denied hitting', *Business Standard*, 14 May 2025, accessed 19 May 2025 https://www.business-standard.com/video-gallery/general/all-about-kirana-hills-which-india-denied-hitting-177288.htm

[22] News Desk, 'Mockery of India's Image...' US-Brokered Ceasefire Triggers Outrage on Social Media', *Mathrubhumi*, 10 May 2025, accessed 15 May 2025https://english.mathrubhumi.com/news/india/mockery-of-indias-image-us-brokered-ceasefire-triggers-outrage-on-social-media-t7r6pkmr

[23] Rahul Harmon, Upasna Singh, and Manish Khatkar, 'Cyber and Electronic Warfare in Context of Defence Forces in Present Scenario', *IEEE Xplore*, 2023, accessed 10 May 2025 https://ieeexplore.ieee.org/document/10157307

[24] Jason Lange and David Shepardson, 'Most Americans See TikTok as a Chinese Influence Tool', *Reuters*, 01 May 2024, accessed 05 May

2025 https://www.reuters.com/world/us/most-americans-see-tiktok-chinese-influence-tool-reutersipsos-poll-finds-2024-05-01/

[25] Shivam Kumar, ;Chinese Soft Power Projection: The Role of Confucius Institutes in South Asia', *Indian Council of World Affairs*, 06 Sep 2024, accessed 05 May 2025 https://www.icwa.in/show_content.php?lang=1&level=1&ls_id=11746&lid=7154

[26] Deeptiman Tiwary, 'NYT Report: US-Based Pro-China Network Funded Indian Website', *The Indian Express*, 08 Aug 2023, accessed 18 May 2025 https://indianexpress.com/article/india/nyt-report-us-based-pro-china-network-funded-indian-website-8881501/.

[27] *International Journal of Kashmir Studies*, vol. 5, no. 1 (Jan–Jun 2023), accessed 17 May 2025 https://kprijk.org/wp-content/uploads/2023/07/IJKS-Vol.5-Issue-01.pdf

[28] Deanna McLean, 'DeepSeek vs ChatGPT: How Do They Compare?', *Elegant Themes*, 30 Jan 2025, accessed 12 May 2025 https://www.elegantthemes.com/blog/business/deepseek-vs-chatgpt

[29] TOI World Desk, 'DeepSeek: China's AI Silent on Tiananmen Square Massacre and India's Control on Arunachal Pradesh', *The Times of India*, 30 Jan 2025, accessed 14 May 2025 https://timesofindia.indiatimes.com/india/deepseek-chinas-ai-silent-on-tiananmen-square-massacre-indias-control-on-arunachal-pradesh/articleshow/117721916.cms

[30] Simon Heron, 'Five Notable Examples of Advanced Persistent Threat (APT) Attacks', *Get Safe Online*, accessed 31 May 2025 https://www.getsafeonline.org/business/blog-item/five-notable-examples-of-advanced-persistent-threat-apt-attacks/

[31] Alexander S Gillis, 'WannaCry Ransomware', *TechTarget*, accessed 31 May 2025 https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

[32] Anneke Smith, ‘Zhenhua Data Leak May Be Typical Contacts List – Tech Expert’, *RNZ*, 17 Sep 2020, accessed 10 May 2025 https://www.rnz.co.nz/news/national/426251/zhenhua-data-leak-may-be-typical-contacts-list-tech-expert

[33] Krishna Patel, P Ashok, Abhijit Chirputkar, and Samaya Pillai, ‘Cybersecurity Risks and Countermeasures in the Threat Landscape of IoT Devices’, paper presented at the *2024 International Conference on Cybersecurity and Threat Intelligence (ICTI)*, 13-15 Nov 2024, published 21 Jan 2025, accessed 30 May 2025 https://ieeexplore.ieee.org/document/10841210

[34] ‘Pakistani Hackers Attacked 1.5 Million Plus Indian Websites after Operation Sindoor’, *The Times of India*, 14 May 2025, accessed 20 May 2025 https://timesofindia.indiatimes.com/technology/tech-news/pakistani-hackers-attacked-1-5-million-plus-indian-websites-after-operation-sindoor-failure-rate-names-of-7-pakistani-hacker-groups-techniques-used-and-more/articleshow/121128592.cms

[35] Maulik Pathak, ‘Gujarat ATS Arrests 18-Year-Old for Cyberattacks during Operation Sindoor’, *Hindustan Times*, 20 May 2025, accessed 21 May 2025 https://www.hindustantimes.com/india-news/gujarat-ats-arrests-18-year-old-for-cyberattacks-during-operation-sindoor-101747755245180.html

[36] Mithun Sarkar, ‘Information Warfare’

[37] Ibid.

[38] Ibid.

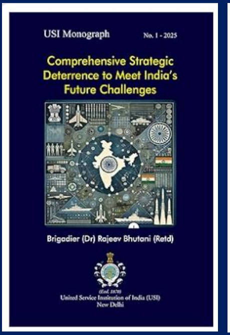
[39] Ibid.

About the Author

Lieutenant General DP Pandey, PVSM, UYSM, AVSM, VSM (Retd) is a former Commandant, Army War College. He was commissioned into the 9th Battalion, the SIKH LIGHT INFANTRY. Throughout his career, he held various command and staff roles in diverse terrains and operational settings. Notably, he participated in Operation VIJAY (Kargil) in 1999 and commanded his unit in Siachen Glacier and Eastern Ladakh. Later, he commanded a Rashtriya Rifles Sector and a Counter Insurgency Force in Kashmir. Before heading the Army War College, he served as the General Officer Commanding of the Chinar Corps. Additionally, he was the inaugural Director General of the Territorial Army. He holds post graduate degrees from the Defence Services Staff College, Wellington, the National War College in Washington DC, and an MPhil from the National Defence College, New Delhi.

About the USI

The United Service Institution (USI) of India was founded in 1870 by a soldier scholar, Colonel (later Major General) Sir Charles MacGregor ‘For the furtherance of interest and knowledge in the Art, Science and Literature of National Security in general and Defence Services, in particular’. It commenced publishing its Journal in 1871. The USI also publishes reports of its members and research scholars as books, monographs, and occasional papers (pertaining to security matters). The present Director General is Major General BK Sharma, AVSM, SM** (Retd).

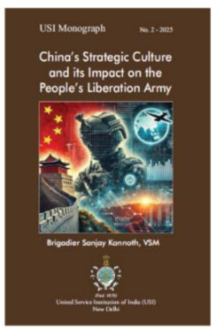


USI Monograph No. 1 - 2025

Comprehensive Strategic Deterrence to Meet India’s Future Challenges

Brigadier (Dr) Rajeev Bhutani (Retd)

(Estd. 1870)
United Service Institution of India (USI)
New Delhi

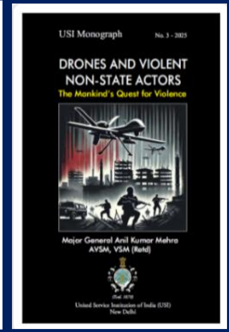


USI Monograph No. 2 - 2025

China’s Strategic Culture and its Impact on the People’s Liberation Army

Brigadier Sanjay Kannoth, VSM

(Estd. 1870)
United Service Institution of India (USI)
New Delhi

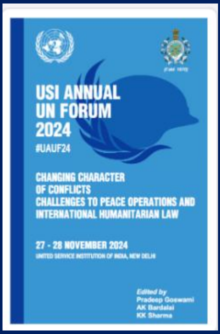


USI Monograph No. 3 - 2025

DRONES AND VIOLENT NON-STATE ACTORS
The Mankind’s Quest for Violence

Major General Anil Kumar Mehra AVSM, VSM (Retd)

(Estd. 1870)
United Service Institution of India (USI)
New Delhi



USI ANNUAL UN FORUM 2024
#UAUF24

CHANGING CHARACTER OF CONFLICTS
CHALLENGES TO PEACE OPERATIONS AND INTERNATIONAL HUMANITARIAN LAW

27 - 28 NOVEMBER 2024
UNITED SERVICE INSTITUTION OF INDIA, NEW DELHI

Edited by
Pradeep Goswami
AK Bardalai
KK Sharma

Rao Tula Ram Marg, Opposite Signals Enclave, New Delhi-110057

Tele: 2086 2316/ Fax: 2086 2315, E-mail: dde@usiofindia.org