CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 198 November 2019

Grey Zone Conflicts and Informationisation in the Indian Context: Challenges, Capabilities, and Way Ahead

Poshuk Ahluwalia was commissioned into the Mechanised Infantry and is a graduate of the Defence Service Staff College (DSSC), Wellington. The Officer has operational experience in CI/CT operations in Jammu and Kashmir and has served in High Altitude Areas of Ladakh. He has also served in a United Nations Peace Keeping Mission. He has been a distinguished pistol shooter having won several medals at various international and national level competitions.

Key Points

- Grey Zone Warfare has been in vogue since the dawn of warfare; however, it has become more pronounced in recent years.
- Belligerents may have different perceptions of their struggle and often employ more than one dimension of national power to achieve national objectives.
- On the peace-war spectrum, Grey Zone Conflict falls between peace and the 'red lines' established by each nation or military alliance to define conditions that justify going to war.
- The essence of informationisation is attacking the enemy's cognitive networks, understanding and convictions; thus, forcing it to give up all resistance and terminate the war.
- Western theatre command of the People's Liberation Army (PLA) is endowed with formations having non-kinetic capability including the electronic warfare (EW), information warfare (IW), communication, and intelligence for the employment in the non-contact phase of the battle.
- To combat the growing complexity of the armed conflict in the grey zone, the Indian Army must explore new ways to utilise its forces.
- Grey Zone War requires the whole government approach whereby ensuring unity of efforts, resulting in simultaneity, and synergised efforts.
- The Indian Armed Forces have made considerable progress in establishing command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks. Since these are predominantly single service specific, it remains a major challenge.
- A limited war does not imply limited capabilities; it refers to the optimum use of specific capabilities at one's command. The need is for highly mobile, well-equipped and versatile forces, capable of multi-dimensional, non-linear missions.

> This is another type of war, new in its intensity, ancient in its origin—war by guerrillas, subversives, insurgents, assassins, war by ambush instead of by combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him....
>
> – President John F. Kennedy,
> *Remarks at West Point, 1962*

Introduction

Based on the lessons of the Vietnam War, Colonel Arthur Lykke Jr, a US Army War College Professor and a retired Army Officer, articulated that 'strategy' is as an equation of "ends, ways, and means," and that "military strategy must support national strategy and comply with national policy."[1] It was an open-ended definition, implying a variety of ways and means to be used to serve its national interest. Around the same time, the Chinese generals and their Russian counterparts studied the First Gulf War (1991) and the precision strike,

Grey Zone Conflicts and Informationisation in the Indian Context: ...

intelligence, surveillance, and reconnaissance capabilities of the United States (US). They also "sought ways to reap some of the political and territorial gains of military victory without crossing the threshold of overt war."[2] Thus, this is how the Chinese and the Russians came up with the concept of 'Grey Zone' so that they could take certain aggressive actions without really escalating the situation into an open confrontation.[3] It means that the environment would be so orchestrated that it remains reasonably ambiguous to prevent any actions by the targeted structures or population. A study of military history suggests that the Grey Zone concept has been in vogue since the history of warfare itself, albeit in different forms. However, it has become more pronounced in recent years.

Rapid changes in the geo-politico-economic landscape and revolutionary changes in technology have ushered in an era of complexity and uncertainty in the security environment. Also, the character of conflict has continued to evolve on account of inter-related changes in the capabilities, circumstances. and motives of the nation states. Considering the global geo-strategic environment, under the shadow of nuclear weapons, the probability of all-out wars between the global powers is low. However, given the unresolved territorial and boundary disputes in the Indian subcontinent and the declared policy wherein no loss of territory is acceptable, the probability of limited conflicts is reasonably high. However, they would have the potential to spill over into a major conflict with hybrid contents. The countries may employ a combination of conventional, unconventional, non-contact methods or rely entirely on unconventional tactics against the relatively strong opponent(s). David Carment argues that in cases where opponents are in asymmetric conflict, states are likely to rely heavily on unconventional tools and covert operations.[4]

Grey Zone

Grey Zone Conflict

In the current scenario, the lines between political, military, economic, diplomatic, intelligence, and criminal means of aggression are becoming increasingly blurred as belligerents more often than not employ more than one dimension of national power to achieve national objectives. The Grey Zone, with hybrid threats, is a metaphorical state of being between war and peace, where an aggressor's objective is to make either political or territorial gains, or both, without crossing the threshold of open warfare with a powerful adversary. The "zone" essentially represents an operating environment in which aggressors use ambiguity and leverage non-attribution to achieve strategic objectives while limiting counteractions by other nation states. Grey Zone's success depends on patience and an ability to covertly blend all the instruments of state power such as Diplomatic, Information, Military and Economic (DIME). The non-military forms of national power are often applied covertly well before the existence of a definable state of open warfare. Centralised, authoritarian governments have a major advantage in synchronising all of the instruments of national power. For example, Russia's President Vladimir Putin maintains strict control over the political, economic, and information functions of the state, providing him with the ability to marshal these elements toward specific strategic goals. Liberal democracies have a major disadvantage because they lack the necessary government centralisation over the economic and informational domains to synchronise them adequately towards military-like objectives without undermining the liberal nature of the state.

The Grey Zone Conflict involves activities directed toward the accomplishment of ends by utilising all methods short of declared war. On the peace-war spectrum, the Grey Zone Conflict falls between peace and the 'red lines' established by each nation or military alliance to define conditions that justify going to war. This strategy allows a less powerful opponent to achieve its objectives without provoking its target into an undesirable or unwinnable war. A key aspect of the Grey Zone Conflict is that it should be sufficiently ambiguous to leave targets unsure of how to respond.[5] This is exactly what the Chinese achieved in progressively securing the islands in the South and East China Seas, and the Russians in annexing Crimea and destabilising Ukraine in 2014. Hal Brands of the Philadelphia-based Foreign Policy Research Institute argues that the Grey Zone tactics are "frequently shrouded in misinformation and deception, and are often conducted in ways that are meant to make proper attribution of the responsible party difficult to nail down."[6] They are drawn from a comprehensive toolset that ranges from cyber attacks to propaganda and subversion, economic blackmail and sabotage, sponsorship of proxy forces and creeping military expansionism.[7]

Moreover, though the term Grey Zone Conflict is new, it bears similarity to other relevant concepts of warfare. These concepts include asymmetric warfare, political warfare, ambiguous warfare, irregular warfare, hybrid warfare, and military operations other than war. The amalgamation of these methods of warfare into one expansive category demonstrates the complexity inherent in all types of conflicts. Not every war fits neatly into one category; rather, each war expresses elements of several theories of warfare. Hence, due to the complex, ambiguous, and evolving nature of this phenomenon, the Grey Zone Conflict should be described

by its underlying characteristics and context and not defined as the sum of its parts.[8] For instance, China has been increasingly engaged in unconventional operations to dilute American hegemony especially in the South China Sea as the unconventional strategies employed fall mostly outside the purview of treaties, international laws, and norms; thus, placing few restrictions on their use. Similarly, emphasis on covert operations and non-military tactics is evident in Russia's actions in the Baltics, Eastern Ukraine and Crimea, which distinctly fall under the purview of Grey Zone Conflict. Since 1989, proxy war cum cross border terrorism in Jammu and Kashmir (J&K) by Pakistan is yet another example of the Grey Zone Conflict syndrome, wherein Pakistan sponsored terrorism has remained below the threshold of open war.

Factors Influencing Grey Zone Conflicts

Participants in the Grey Zone Conflict may have different perceptions of their struggles that motivate them and influence their actions. An antagonist may wage a limited conflict, while the protagonist believes he faces an existential threat. These perceptions may run the full gamut of peace and war thus making it more difficult to understand and respond to the situation. India, today is increasingly vulnerable to threats that are spread across a wide spectrum ranging from societal and cultural to geostrategic and military. Under such circumstances, how does a Grey Zone emerge? The factors fuelling the emergence of Grey Zone conflicts are discussed as under:[9]

- **Societal and Structural Conditioning:** Intending to create societal space for conflict, the population of disputed areas have to be made to believe that they are an oppressed class.
- **Psychological Conditioning for the Employment of Non-State Actors (NSAs) in J&K:** Attempts have been made to legitimise the employment of Non-State Actors (NSAs) and terrorists by creating a perception that they are fighting for a just cause. Moreover, those resisting separatists and terrorist organisations in J&K have been portrayed as traitors by the NSAs and the terrorists.
- **Secondary Coercion:** Terrorist attacks on the security forces, in other parts of the country, and even against the local population are means to coerce the people into supporting them and joining the so-called "people's movement" if the support does not come willingly.
- **Subversion:** The full potential of hybrid tactics in the Grey Zone can be realised if there are a gradual erosion and ultimate collapse of governance and state institutions. Hence, targeting educational institutions to propagate secessionist ideology cannot be ruled out.

Potent Tactics in the Grey Zone

The factors that increase the efficacy of Grey Zone operations are as follows:

- **Simultaneity and Multi-Modality of Application:** The Grey Zone Warfare is effective if components across the entire spectrum are employed simultaneously in the same battlespace. In such cases, the employment of military, political, diplomatic, and cyber capabilities is imperative.
- **Subversion of Governance:** Grey Zone operations can completely destabilise a nation. Syria, Iraq, and Afghanistan imploded primarily because of subversion and fragmentation of society and the resultant denial of space-to-state institutions.
- **Information War:** Information War is a potent tool to influence or mould the perception by way of misinformation and disinformation campaign against the adversary.
- **Resource-Control:** Denial of access to resources weakens the war-waging capability of the target nation. Denial of resources is achieved by disrupting communications and destroying resources. The other aspect of resource-control is the exploitation of resources for enhancing capabilities. Islamic State (IS) had both denied resources to Syrian and Iraqi governments and used the same resources to enhance its capabilities.
- **NSAs and Irregulars Acquiring Conventional Capabilities:** Hezbollah, Syrian Democratic Forces (SDF), and IS have acquired conventional and sub-conventional capabilities. It is not possible to acquire such capabilities without state patronage. Such groups pose a serious threat when combined with other tools of war. Terrorists with conventional capabilities getting support from irregulars and regular forces from across the borders are a serious threat to national security.
- **Multi-Actor Battle Space:** Irregulars such as tribal raiders and NSAs can operate both as terror organisations and with the regular forces. Prominent examples would be the Hezbollah and the SDF who have acquired the capabilities to operate both as regulars and NSAs. The targets of regulars, criminals, and irregulars could be different. Irregulars could target regulars, terrorists could dominate the cognitive domain, and criminals could target those whom they consider as obstructing their larger goal. Their synergised application would pose a serious challenge.

Future Global Scenario: An Uncertain Future

While full-scale warfare remains unlikely, powerful nations are likely to continue to exploit the Grey Zone between war and peace to remain dominant and ensure their status as world powers. For states unprepared for this mode of warfare, the challenge will be to prepare to counter subtle aggression in the littorals, where aggressors will increasingly deploy non-military anti-access measures. The need of the hour is for responsible states to continue to work towards an environment which is based on the primacy of international laws and treaties. At the same time, regional powers must be prepared to operate and fight in conditions of increased ambiguity, leveraging all the instruments at their disposal.

Informationisation

It may be realistic to presume that any war of the future in our context is more likely to be limited in scope, and thus limited in time and space. Nonetheless, it will be marked by high tempo and lethality and may be fought across the entire spectrum of conflict including informationisation. In the development of this concept, one of our potential adversaries China has the capability to mobilise and deploy a sizable force against India in high threat scenarios, should it want to activate the entire border. Its latest doctrine of "winning local wars under conditions of informationisation" lays stress on network-centric warfare, cyber warfare, acquisition of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4I2SR) systems, pre-emption, surprise, and deception as also the employment of Special Forces. It has taken a lead in our neighbourhood and it has now entered an era where informationisation is the military concept of the present and future.

China's Informationisation

Informationisation "entails embracing all the opportunities and technologies the Information Age can offer and integrating them into military systems".[10] It (*xinxihua* in Mandarin) means that information technologies (ITs), especially those capabilities relating to C4ISR are considered supreme to expanding military effectiveness.[11] This entails, dominating the electromagnetic spectrum through integrated network electronic warfare as well as exploiting technological advances in microelectronics, sensors, propulsion, stealth, and especially cyber to outfit the People's Liberation Army (PLA) with new capacities for long-range strike and disruption. Information Warfare (IW) is a subset of informationisation. China's 2004 White Paper on National Defence outlines the importance of informationisation. In short, the PLA, in its long transition from People's War to limited local wars under conditions of informationisation, was seeking to move from being a platform-centric to a more cyber-enabled force, or one where the crucial characteristic of the force is the network linkages among platforms, as opposed to the platforms themselves. PLA's most recent Defence White Paper, "Chinese Military Strategy," published in May 2015 places an even greater emphasis on informationisation and makes it central to operational concepts.[12] Through Defence White Paper, PLA seeks to fully develop its capabilities in all dimensions of warfare including the electromagnetic spectrum with an aim of fighting and winning "Informationised local war".[13]

Chinese Threat

The examination of the PLA's capabilities given the requirements of informationised local war demonstrates that wide gaps still exist. To begin with, despite the tremendous technological leap of the PLA during the last decade, it is probably still beyond China's capability and will to equip its entire military forces with state-of-the-art weapons and equipment. A gap between those capabilities and a full-scale informationised war still exists, and the extent to which China will be able to bridge it depends on six variables, i.e. three exogenous and three endogenous. Exogenous variables include the timing of the war, its scale and the capabilities of the adversaries. The longer China can prepare, the more limited the war is, and the less sophisticated the enemies are, the more capable PLA will be of conducting a local war under conditions of informationisation.

Regarding the other set of variables which are endogenous in nature, what determines China's competence to wage such a war is consolidating a systematic military doctrine that consists of a clear and consensual threat perception, adopting a procurement policy that acknowledges China's financial and technological limitations and overcoming the bureaucratic and political barriers that prevent PLA from undertaking the structural adjustments that its doctrine demands. As for the last factor, it seems that despite its prime importance it has received the least attention. Nevertheless, all that is set to change with theatre commands having come up and all elements of military forces being directly under one single commander. Important challenges continue to face the PLA in the area of jointness and efficiency. Optimising the fighting force to undertake combined arms warfare is a hurdle and remains a critical weakness.[14]

Likely Goals of China's Informationised Warfare

Chinese experts believe that IWs essence is the sum of information capabilities that can break the will to resist by attacking the enemy's cognitive understanding and convictions, forcing it to give up all resistance and terminate the war. In the military sense, this means overall use of various types of ITs, equipment and systems, particularly his command systems, to shake the determination of enemy's policymakers and at the same time, the use of all means possible to ensure that one's systems are not damaged or disturbed. This would largely be consisting of five major elements mentioned as follows:[15]

- **Substantive Destruction:** The use of hard weapons to destroy enemy headquarters, command posts and command and control (C2) information centres.
- **Electronic Warfare:** The use of electronic means of jamming or the use of anti-radiation (electromagnetic) weapons to attack enemy information and intelligence collection systems such as communications and radar.
- **Military Deception:** The use of operations such as tactical feints (simulated attacks) to shield or deceive enemy intelligence collection systems.
- **Operational Secrecy:** The use of all means to maintain secrecy and keep the enemy from collecting intelligence on our operations.
- **Psychological Warfare:** The use of TV, radio, and leaflets to undermine the enemy's military morale.

Implications for India

Of all the five theatre commands, the most vast and crucial Western theatre command of the PLA is deployed along the Sino-Indian border. The Theatre is endowed with formations having non-kinetic capability including EW, IW, communication, and intelligence. It is these non-kinetic means that will form the mainstay of the likely future conflict in the non-contact phase of the battle. The likely concept of operations of the PLA during a limited conflict under conditions of informationisation as hinted in the White Paper would be to:

- Achieve strategic deception and stage-manage build-up of own troops.
- Shape the environment and battlefield to own advantage.
- Create a decision-dilemma for the enemy by multi-dimensional, multi-spatial engagements.
- Ensure the simultaneous and non-linear application of forces.
- Retain control over escalation and exit-strategy.
- Endeavour to achieve the desired end-state well before reaching the culmination point.

Way Ahead for India

The Indian Army trains, organises, and equips itself to fight large-scale, conventional wars that pose an existential or significant threat to the nation or its interests. Our war fighting concepts, along with experience in war establish a mindset that favours mass, offensive tactics, and the pursuit of short, decisive victories. This way of thinking continues to hold sway despite our increasing involvement in proxy war and limited conflicts. The Indian Army understands that the future battlefield which will be volatile, uncertain, complex and ambiguous, and would be driven by technology. The reforms to make the force modular, agile, and leaner are already underway to prepare it for conflicts of the future.

To combat the growing complexity of armed conflict and the Grey Zone competition, the Indian Army must explore new ways to utilise the force it has. Army leadership may employ conventional forces to effect positive change across the entire spectrum of conflict, from the Grey Zone to theatre-level wars. While the solution to any conflict is a whole-of-government approach, conventional forces may have opportunities for an expanded role in Grey Zone conflicts given the appropriate training, experience, and organisation.

Threats in the Grey Zone Need a Response in the Grey Zone

Grey Zone is not purely a military matter; it is a war against a nation, a society, a culture, and its people. To deal with this emerging threat, the national approach is required. We should not look at this form of warfare purely through the prism of conventional military response. It would be highly incorrect to do so. The response requires a strategy and synergy between military and non-military partners and other law enforcement agencies. Some of these response strategies are discussed next:

- **The Need for Unified Effort:** The Grey Zone War requires the whole government approach to deal with it. The response should be based on the principle of unity of efforts, simultaneity, integrated, and synergised approach. Execution of the plan should be coordinated at the highest level to achieve cooperation for the effect-based response. Tools such as diplomatic, cyber,

informational, economic, political, asymmetric, and military must be employed. The idea is that the operational commanders cannot achieve strategic objectives solely through military action but must depend on the full government response to achieve appropriate goals. Thus, the defining principle of dealing with the Grey Zone War is "unified effort" simultaneous application of tools of war, "mixed tactics" conducted across the enemy's territory, and more importantly, within its "spheres of influence".[16, 17]

- **Single Command Authority—A Pre-requisite:** A synergised response under a single command authority covering both military and non-military measures is imperative for success in the Grey Zone. Intelligence agencies are operating independently of the security forces and are not responsible for the troops on the ground. The Ministry of Home Affairs (MHA) controls the Central Armed Police Force whereas the Army operates under the Ministry of Defence (MOD). The State Police and the India Reserve Battalions (IRB) operates under state authority. Cyber and information war is conspicuous by its absence and even if it is being initiated, it is independent of the other agencies. Therefore, the fragmented approach, in the absence of a common operational plan, is unlikely to achieve the desired results. There is no single central authority that is responsible and accountable for the execution of a comprehensive and integrated response.
- **The Need for a New Doctrine for Integrated Action:** Strategies for war are conceptualised during peace time. The Grey Zone War is complex and the military needs to define its strategy, doctrine, concept of operations, force restructuring, special equipment, and special training. It would require combatants and non-combatants as part of the force, to deal with every element of the Grey Zone War.
- **The Relevance of Conventional Capabilities in the Grey Zone War:** The Indian Armed Forces are equipped, trained, and structured to fight conventional wars. Often the question, that arises, is that if India is unlikely to fight a conventional war then why so much focus on conventional capabilities? The simple answer is that if India does not maintain its conventional capabilities it will be engaged in sub-conventional and hybrid war at multiple levels. Conventional deterrence therefore will have to be maintained. However, one should not also assume that all state-based warfare will be entirely conventional.[18]
- **Time and Place to Engage:** It is a smart strategy to determine when and where to fight. There is a need to identify the tools that are to be applied at a particular stage and against what specific threat. The cyber threat can be handled by the cyber as well as the law enforcement authorities. The tools should be determined by strategy and not as an emergency response.
- **Intelligence Agencies as First Firewall:** Intelligence agencies are required to carry out the mapping of the human terrain and the social, economic, and cultural fault lines. The "mapping of human terrain" requires intellectuals, social scientists, cyber experts, information warriors, and professionals to understand and unravel any erratic behaviour by individuals and/or groups of people. Thus, the first responders should be intelligence agencies, law enforcing agencies, and state administration.

Informationisations and Own Response Strategy

The Indian Armed Forces have made considerable progress in establishing C4ISR networks. But given that these are service-specific, there is a need for establishing a Joint Inter-Services Network. The other areas that need attention are as follows:

- In the era of cyber warfare, IW, and net wars, information systems, both civil and military networks, should have adequate redundancy, survivability, and electronic security.
- For optimisation, the strengths of our IT infrastructure and industry and advancements in satellites and radio-based systems should be jointly exploited by the military and civil sectors. Further, our dependence on Chinese IT hardware needs to be reduced significantly.
- Joint network and individual services networks should be able to function in all environments including the nuclear overhang. For instance, they should be hardened against or be resistant to a nuclear electromagnetic pulse (EMP) attack.
- We need to induct a wide variety of military satellites for upgrading our strategic Intelligence, Surveillance, Reconnaissance (ISR), Signals Intelligence (SIGINT), Electronic Intelligence (ELINT), Communications Intelligence (COMMINT), imagery and navigation capabilities.
- Even though Computer Emergency Response Teams (CERT) at national and lower levels have been formed to respond to cyber attacks on civilian infrastructure, the concept is more defensive in nature. A pro-active concept like that of net force may be more appropriate with considerable offensive capability.

Recommendations for Capability Building

The Grey Zone Warfare and Limited Conflict under conditions of informationisation will require building capability across the entire spectrum of comprehensive national power (CNP). This requires a deep sustained approach which should include all the elements of national power. The aim should be to enhance their potential of real-time employment, when required, to maintain deterrence under all circumstances, be it conventional or unconventional and even limited or escalatory. India needs to progressively build the capability of hard military power, soft power, and demonstrated power in its quest to be recognised as a regional power with global influence, which can deter threats to its stability and integrity. The Army, being the largest component of the Indian Armed Forces, must be prepared to play its mandated role in the interests of defence and security of the country. Some of the measures that need to be put in place are mentioned next:

- **Deterrence Posture:** The Indian Army's deterrence posture must be based on flexible capability-based structures to deal with various forms and levels of conflict. It requires upgraded technology with pre-dominant capabilities for prosecuting hybrid, conventional, and informational wars under a nuclear overhang. We must develop retaliatory counter sub-conventional threat capability within existing resources by raising the Special Forces Command.
- **Transformation and Right-Sizing:** The Indian Army needs to undergo transformation and right-sizing towards becoming an optimised modern force, with a more efficient teeth-to-tail ratio. It would make more pragmatic and economic sense to have only a minimum essential capability on either front while maintaining a suitably large dual-front capable central reserve, possibly under the aegis of a Strategic Reserve Command to reinforce the front where the actual threat develops.
- **Theatre Commands:** The appointment of a Chief of Defence Staff (CDS) has been approved by the government. However, the formation of 'theatre commands' would contribute to the optimisation of resources and ensure unity of command.
- **Defence Budget:** The government must increase allocation for defence (excluding pensions) to 2.5 percent of the gross domestic product (GDP) initially, and further raise it gradually to 3 percent that too only on a year-on-year basis and until the modernisation of the Armed Forces is complete. Concurrently, the government must introduce a system of 'roll-on' budget, whereby funds once allotted to defence cannot be re-appropriated for any other purpose.
- **Future Ready Structures:** New structures for expanding the Army Aviation, enhancing informational warfare capability and raising the Special Operations, Cyber and Space Commands must be undertaken at the earliest.
- **National Security Strategy:** The government must guide the military through the issuance of national security strategy, defence policy, and military strategy so that the three services, including the Army, can align their respective policies and doctrines to these directives in a coordinated manner.

Conclusion

India needs to be prepared to combat Grey Zone threats and needs to be aware of it so that it does not become a victim of such threats because of its negligence. There is a need to introspect, analyse, and formulate the doctrine and strategies to have an effective mechanism to deal with it. The Grey Zone Warfare will be a defining feature of the future security environment and thus a fragmented approach will be detrimental to the national interests. The debate of ethics and rules does not apply to the Grey Zone War. What is important is the impact of own response to a borderless war. As Frank Hoffman states:

Tomorrow's conflicts will not be easily categorised into conventional or irregular, the emerging character of conflict is more complicated than what it appears. A binary choice of big and conventional versus small or irregular is too simplistic.[19]

India needs to develop an understanding of the Grey Zone War and the contours of conflict suggest that the future wars will not be completely conventional, nor should it be assumed that state-based conflict has passed into the dustbin of history. State-based conflict is less likely, but it is not extinct. An essential aspect of dealing with limited wars would be the crucial need to control the escalatory continuum so that the situation does not escalate to unforeseen or unplanned levels. This will have to be done in conjunction with the other instruments of our Comprehensive National Power, more specifically in the diplomatic realm.

To conclude, it may be mentioned that in the emerging security paradigm, where future wars may be limited in scope and time, new thinking is essential.[20] However, it needs no emphasis that a limited war does not imply limited capabilities; it refers to the optimum use of specific capabilities at one's command. The need is for highly mobile, well-

equipped and versatile forces, capable of multi-dimensional and non-linear missions. There needs to be greater emphasis on the exploitation of technology, operational and tactical mobility, precision fire power, and network centricity at all levels. Related to this, there would be a need to map future battlefields in the Indian context so that our Forces are prepared for all possible contingencies. The necessity for a whole of government approach in such operations has been well-established and must be duly ensured.

Notes

1. Arthur F. Lykke, *Military Strategy: Theory and Application*, US Army: Washington, 1993.
2. *The Economist*, "Shades of Grey: Neither War Nor Peace", 25 January 2018, p. 43, available at https://www.economist.com/special-report/2018/01/25/neither-war-nor-peace, accessed on 25 September 2019.
3. Ibid.
4. David Carment, "War's Future: The Risk and Rewards of Grey Zone Conflict and Hybrid Warfare", *Canadian Global Affairs Institute*, October 2018, available at https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare, accessed on 2 September 2019.
5. *The Economist*, 2018, p. 44.
6. Hal Brands, "Paradoxes of the Gray Zone", *Foreign Policy Research Institute, Center for Security Studies*, 27 December 2016, available at https://css.ethz.ch/en/services/digital-library/articles/article.html/01236d5a-cd51-4c3f-a032-4e395339c696/pdf, accessed on 25 September 2019.
7. *The Economist*, 2018, p. 43.
8. Nicholas M. James III, "US Army Conventional Focus in Gray Zone Conflict", School of Advanced Military Studies, United States Army Command and General Staff College, Monograph, 15 March 2017, Kansas, available at https://apps.dtic.mil/dtic/tr/fulltext/u2/1039016.pdf, Accessed on 26 September 2019.
9. Narender Kumar, "War Beyond Rules: Hybrid War and India's Preparedness", *CLAWS Journal*, Summer 2017 Issue, pp. 58-74.
10. Richard A. Bitzinger, "China's Informationised Warfare': Impact on the Region", S. Rajaratnam School of International Studies, RSIS Commentary, February 2016, available at https://www.files.ethz.ch/isn/196258/CO16045.pdf, accessed on 25 September 2019.
11. Ibid.
12. Richard A. Bitzinger, "China's Love Affair With 'Informatized Warfare", *Asia Times*, 27 February 2018, available at https://www.asiatimes.com/2018/02/opinion/chinas-love-affair-informatized-warfare/, accessed on 25 September 2019.

    Kartik Bommakanti and Ameya Kelkar "China's Military Modernisation: Recent Trends", Observers Research Foundation, Issue Brief, 26 March 2019, available at https://www.orfonline.org/research/chinas-military-modernisation-recent-trends-49284/, accessed on 26 September 2019.
13. Ibid.
14. Ibid.
15. Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare", Vol. 30, Issue 4, October 2006, available at https://idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare_vanand_1006, accessed on 25 September 2019.
16. Op. Cit. (12).
17. Gary Luck and Mike Findlay, "Joint Operations Insights & Best Practices", *Joint Warfighting Centre*, United States Joint Forces Command, July 2008, 2nd Edition.
18. Frank Hoffman, "Hybrid Warfare and Challenges", *Small Wars Journal*, JFK,, Issue 52, 2009, available at https://smallwarsjournal.com/documents/jfqhoffman.pdf, accessed on 26 September 2019.
19. Ibid.
20. General Deepak Kapoor, "Limited Wars in the Indian Context", *India Strategic*, February 2012, available at https://www.indiastrategic.in/topstories1368_limited_wars_in_the.htm, accessed on 26 September 2019.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in
CLAWS Army No. 33098