IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

COUNTERING GREY ZONE THREATS DURING CONVENTIONAL MILITARY OPERATIONS

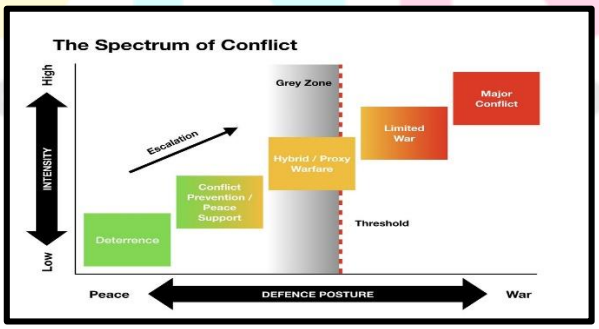
The categories of warfare are blurring and no longer fit into neat, tidy boxes. One can expect to see more tools and tactics of destruction - from the sophisticated to the simple - being employed simultaneously in hybrid and more complex forms of warfare. - Robert M. Gates, Former US Secretary of Defence[1]

Upendra Kumar Srivastava
Indian Army, Jammu, India

Abstract: *This article aims* to analyze the potential grey zone threats to India from its belligerent neighbours in the West and North. Besides, it also endeavours to suggest measures that India should adopt for its kinetic and non-kinetic military operations. Apart from the same, an attempt has been made to define grey zone threats from the Indian perspective. Till recent times grey zone threats were getting blurred with the concept of hybrid threats and fifth and sixth-generation warfare. It's ironic that even after more than seven decades of independence, four full-fledged wars and ongoing low-intensity conflicts in border states, India is reactive to these threats. Though, certain major steps are being taken by the present dispensation of the country, but it is too little to match China in this domain.

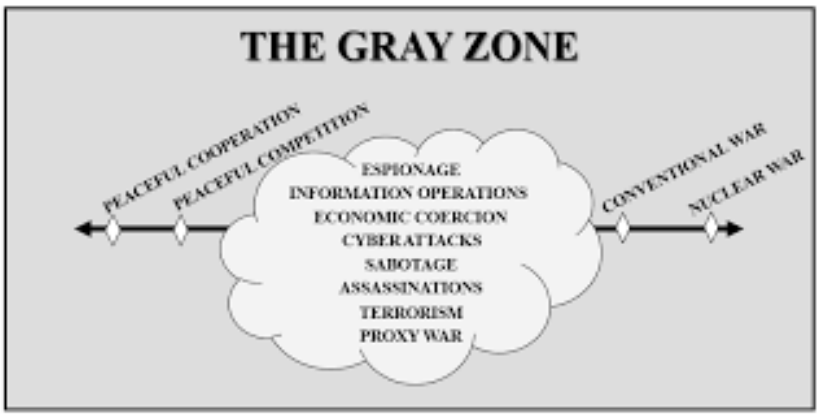
INTRODUCTION.

Defining Grey Zone Conflicts To lay the groundwork for suggestions to counter Grey Zone threats in a conventional operation and during No War No Peace (NWNP) it is important to define and understand the concepts of Grey Zone aggression. The aim of this article is not to assess the phenomenon of grey zone conflict in and of itself, but to propose alternatives for dealing with it during a conventional war. Nonetheless, it is important to underscore the critical nature and possible manifestation of this challenge in order to lay the groundwork for developing response options to combat India's conventional threats, particularly China and Pakistan. According to the United States Department of Defence, the Grey Zone is the strategic space between statecraft during peace and total war, which occurs when countries or actors deliberately use all available aspects of authority to achieve politico-military goals that go beyond the limit of peaceful existence while remaining below the level of all-out overt military confrontation. By questioning, undermining, or breaking international rules, norms, regulations, and customs, these actors endanger each other's interests.



To summarize the above concepts, the Grey zone is an operational zone between peace and war that includes operations to change the status quo below a limit that, in most instances, would trigger a traditional military reaction, sometimes by blurring the boundaries between military and non-military operations and event attribution.

[1] Robert M. Gates, 'A Balanced Strategy: Reprogramming the Pentagon for a New Age', Foreign Affairs, January–February 2009, available at https:// www.foreignaffairs.com/articles/united-states/2009-01-01/balanced-strategy, accessed on 06 February 2021.



NEED OF THE STUDY.

At times hybrid warfare is confused with grey zone conflicts which are distinctly different in terms of concept and their manifestation. To simply understand the difference between the two one needs to go through the definition of the grey zone. It the "Zone or, Domain" between peaceful co-existence and all-out war. And all activities by the aggressor, right from statecraft to the use of kinetic means (ethical/unethical) including hybrid war, are fought in the domain of "Grey". Therefore, Grey-zone conflict may incorporate conventional and non-conventional techniques or rely entirely on non-conventional tactics. Complete reliance on unconventional tools is likely to be less effective at fully and rapidly compelling relatively strong opponent(s) into specific avenues of the desired action. Thus, states engaged in grey-zone conflicts are likely to use hybrid techniques, and more of their conventional resources, when there is a perception that the use of unconventional techniques will not fully achieve the desired outcome. In asymmetric confrontation, where the cost of applying traditional methods against a weaker opponent is much lower, the use of conventional force against an opponent is more likely. States, on the other hand, are likely to rely heavily on unorthodox approaches and covert activities in situations where opponents are engaged in asymmetric conflict. The table below provides a comparison of grey-zone and hybrid warfare characteristics. Our cases relate to situations where asymmetry predominates.

ATTRIBUTES	GRAY-ZONE CONFLICT	HYBRID WARFARE
LEVEL OF ENGAGEMENT	TACTICAL, OPERATIONAL, STRATEGIC	TACTICAL AND OPERATIONAL
USE OF CONVENTIONAL MILITARY FORCE	USED WITH NON-CONVENTIONAL OPERATIONS	USED WITH NON-CONVENTIONAL OPERATIONS WHICH IS GENERALLY A DOMINATING ELEMENT
USE OF NON-CONVENTIONAL MILITARY FORCE	MAY BE USED STANDALONE OR WITH CONVENTIONAL OPERATIONS	USED WITH CONVENTIONAL OPERATIONS AS AUXILIARY TACTICS
DURATION/TIMELINE	PROTRACTED	PROTRACTED OR, SHORT
AIM OF THE AGRESSOR	GLOBAL AND/OR REGIONAL REVISIONIST.	DOESN'T APPLY AS CONCEPT PERTAINS TO OPERATIONAL AND TACTICAL LEVELS.
SYMMETRY BETWEEN OPPONENTS	APPLICABLE UNDER SYMMETRIC AND ASYMMETRIC CONDITIONS	MAINLY USED UNDER ASYMMETRIC CONDITIONS

RESEARCH METHODOLOGY

Several articles and research papers available in the open domain have been read and referred to during the compilation of the article. Apart from the same, some of the service officers working in the field were also contacted for input.

CHARACTERISTICS OF GREY ZONE CONFLICT

- **Level of Aggression** The aggressor's desired level of engagement is one of the most important characteristics of grey zone conflict. Grey Zone aspects are still just on the edge of justifying a military conflict. The aggressors in the Grey zone strive to keep their actions just short of, or even well short of, accepted military action triggers. The objective is to avoid direct conflict, armed confrontations, and direct breaches of international law. This trait will influence the decision to take a specific action, such as cyber-harassment or posing a threat to life by being present in a maritime region. The grey zone perpetrator's plan will be to follow a series of hostile actions with a period of quiet under the guise of normalcy while also manipulating and creating world opinion in its favor about its activities. Grey zone campaigns are thus designed in their relevant activities and overall design to condemn the target precisely the sort of consistency in violation of laws and regulations that is traditionally important in effecting a deterrent.
- **Protracted Period of Manifestation** The ***second*** distinguishing feature of grey zone campaigns is that they evolve slowly and steadily over time, with all-encompassing activities unfolding over time rather than achieving the desired outcome in a single step. As in the case of India and China, the belligerent neighbour has followed a policy of 'sliming slicing' over the years, keeping India short of any decisive responses. India suffers from the same grey zone campaign waged by Pakistan in the garb of the unresolved issue of Kashmir wherein it has been fuelling terror in the valley for the last three decades.
- **Non-Attributability** The lack of transparency and attributability is the ***third*** feature of the grey zone, which extends to some but not all of the operations in this domain. The majority of grey zone operations entail activities in which the aggressor adheres to the principle of deniability and attempts to conceal its role to some extent. For a proxy war, the aggressor will use cyberattacks, misinformation campaigns, or non-state actors, and these operations allow a grey zone

aggressor to deflect reactions from the target country while also blocking potential deterrence - merely by denying responsibility.

- **Historical and Legal Claim** Some grey zone operations are clear and accountable, and they are characterized by a ***fourth*** common facet: the use of pervasive legal and political reasonings, often based on historical assertions backed up by old documentation evidence that suit the aggressor. Nations waging grey zone campaigns go to great lengths to justify their activities under international law. As in the case of China's assertiveness in the South China Sea, where it has been pressuring other nations to support its position despite its fragile legal standing in the global community. Another example of Chinese assertiveness is its actions on the Indo-China border wherein it refuses to accept the legalities of historical documents signed before 1949. In the case of Pakistan, it has been references to the UN resolution of 1947 on Kashmir which was never followed by Pakistan itself. These tactics make it more difficult to develop a local response and impose punitive measures.
- **The policy of Denial** ***Fifth,*** grey zone campaigns traditionally stop short of threatening the defender's vital and existential concerns in order to distract decisive actions. This element, of course, arises from a strategy that keeps response thresholds low, but it deserves special attention. The task of efficient deterrence and reaction is made much more difficult by the defender's refusal to challenge critical interests - particularly when the defender is using extended deterrence, as India is doing against Pakistan - grey zone aggressors. As a result, one of the most distinguishing characteristics of grey-zone campaigns is that they consist of a long series of small successes. They are physical domains or problems where China or Pakistan can fill a power vacuum by daring to respond to India, its allies, and partners. In territorial terms, this could be a feasible possibility, such as when China sends fishing boats to the international waters of the South China Sea based on previous fishing rights claims. Aggressors in the grey zone seek out areas where defenders are unable to respond quickly or aggressively and stake out positions from which they must withdraw, thus shifting the danger calculus to the defender. In other words, grey zone tasks entail a relentless effort to identify and exploit vulnerabilities in the target nation's current policies and capabilities for strategic gain. Any response mechanism, policy, or approach must address the grey zone's essentially unscrupulous, gap-filling nature. It emphasizes the importance of continuous dissuasion in high-priority areas and issues, as well as the ability to move quickly when problems arise. Waiting for the right time to react to an enemy's actions will help the aggressor in the grey zone achieving an early advantage which would be difficult to overcome.
- **Remain within Threshold** The ***sixth*** attribute of the grey zone is that, although it wants to remain below key triggers for punitive action, it employs the threat of escalation as a source of coercive clout, like Pakistan's threat to use a tactical nuclear weapon (TNW) against India. Campaigns in the Grey Zone are intended to remain below the threshold for a large-scale military response, but they still, and somewhat paradoxically, point to the potential of more aggressive military interventions, which would provide momentum for escalation and complicate deterrence concerns. Grey zone conflict targets understand that if they respond violently to a relatively minor movement of the grey zone, the perpetrator can retaliate with more serious capacities, such as military might. China employs such escalating risks in part by positioning maritime militia and coast guard vessels at points of contention with its "grey hull" resources, the People's Liberation Army Navy just above the horizon. China's action in Galwan, in relation to India, is an example of the grey zone campaign's attributes. Coercion is a key component of the grey zone campaigns, and these activities are a prime example of it.
- **All out Efforts by the Aggressor** ***Seventh,*** grey zone campaigns are based on non-military means that stay below critical response limits. To avoid even the appearance of outright military violence, the grey zone perpetrator employs political, informational, cyber, quasi-military forces, militias, and other resources and strategies. To respond properly, defenders must develop parallel statesmanship tools to intimidate or carry out deterrence threats.
- **Target the Fault lines** Finally, Grey zone campaigns are intended to take advantage of specific faults in the countries targeted. Political polarisation, social divisions, unrest waged by ethnic groups (supported by the grey zone aggressor) and economic stagnation are just a few examples. Tacit support and funding to farmers' agitation, CAA protests, and long drawn proxy war in Kashmir are apt examples of the same. Aggressors in the grey zone frequently try to position defenders in conditions where strong answers are either impossible or ineffective for geopolitical and domestic political purposes. Aggressors may achieve this in part by developing economic relations that provide tacit leverage or by attempting escalation. As a consequence, perhaps the most significant feature of the grey zone is that it takes advantage of strategic uncertainty to make incremental gains. Drawing clearer lines where aggression cannot cross thresholds, thereby bounding the issue, is the first step in reacting to grey zone aggression. Only a small subset of grey zone strategies, however, are likely to be capable of doing so. Grey zone strategies are based on the principle that an aggressive state would take several actions below the point where a defender feels secure in making such unambiguous response commitments. The challenge of reacting to such slow aggression is made more difficult by the fact that allies and partners have diverse risk appetites and preferences. Many European countries believe that despite of Russia's approach against the West, keeping good relations with the country is critical in a multipolar world. Similarly, many Asian countries are trapped between China's economic hegemony and their fears about Beijing's coercive moves, making them hesitant to take a firm stance.

GREY ZONE THREATS TO INDIA

India is constantly threatened by its two adversarial neighbors, China and Pakistan. Pakistan has perfected the strategy of "Bleeding India through a Thousand Cuts," recognizing its traditional weakness. Collusion between China and Pakistan in the grey zone is becoming more common, as evidenced by Pakistan's recent activities, such as an attempt to change the status of Gilgit-Baltistan, the conduct of allegedly rigged elections, and the publication of a farce of a map depicting Ladakh and Junagadh as parts of Pakistan. Such activities by Pakistan, in collusion with China, are taking place in flagrant violation of previous treaties and foreign legislation. Similarly, China is using pressure point strategies such as face-offs and salami-slicing along its northern borders, as well as exploiting its economic might to stifle India's economic growth. A recent example is China's attempt to smother India's economy through the ASEAN-sponsored Regional Comprehensive Economic Partnership (RCEP). Inciting Nepal to raise the Limpiyadhura-Kalapani-Lipulekh dispute and Doklam are a few occurrences that can be grouped under the grey zone. Also falling into the grey zone would be China's clever use of maps and old manufactured revenue documents to bolster their claims to territories along the LAC and Borders. There is also a widespread belief that China and Pakistan are the only countries involved in grey zone operations

against India. This isn't completely accurate, though. A number of information activities that fall into the grey zone have been initiated by friendly countries to foster their national interests. The CAA and NRC protests by farmers are a good example. It is a serious threat when certain Western political parties, media outlets, and self-proclaimed human rights rating agencies have been raking India's internal problems in their own country and in front of the world, based on half-baked facts. An in-depth examination of all of these indicates that they are being financed by an adversary of the Indian state, despite the fact that the West is supposed to be the "custodian" of world peace and human rights.

GREY ZONE THREAT DURING CONVENTIONAL OPERATIONS

Although, the very aim of the conflict in 'Grey Zone' is to avoid a direct military confrontation with the opponent by keeping the engagement below the threshold of conventional war. In the preceding paragraphs, we have seen that Grey Zone conflicts are waged against the opponent country for a protracted period of time by employing all possible means in the realms of DIME under the umbrella of the cognitive and non-cognitive domain. But during the prosecution of the Grey Zone conflict, a situation may arise wherein the belligerent country or the aggressor might not be able to control the escalation and the defender country uses conventional means to teach the belligerent a lesson which eventually leads to spiraling off the situation into a full-fledged war. Like in the case of India and Pakistan, such a situation had come up in the year 2001 after the parliament attack which saw the mass mobilisation of Indian Armed Forces known as Operation Parakram. Grey Zone threats and manifestation during a conventional operation are not different from non-conventional operations, rather it would be the extension of ongoing non-contact warfare (NCW) means to support conventional military operations. Some of them are Cyber Warfare, Space Warfare, Information Warfare, Diplomatic Warfare, and Economic Warfare. Therefore, in the case of India Grey Zone threats exist from China and Pakistan during NWNP. During a conventional operation when India faces a contingency from China and Pakistan together it also talks of two and half front wherein the half front will be fought in Grey Zone. All conventional threats from China will be preceded by operations by its PLASSF and PLARF components which will be non-contact warfare. Apart from that before the use of any kinetic means, China will be using diplomatic, informational, and economic means over a protracted period to justify the aggression. In the case of Pakistan, its Grey Zone tactics have been successful in the state of J&K wherein it has used the hybrid elements and religious and ethnic fault lines to keep the pot boiling to serve its stated agenda of "bleeding India by thousand cuts". In a scenario of conventional operations through the UT of J&K, the above-stated fault lines would be detrimental to the Indian security forces, therefore they need to be kept under check.

MEETING THE CHALLENGES OF GREY ZONE

Grey-zone operations are national issues that necessitate national solutions. Relying on the Indian Armed Forces to combat grey-zone activities would be a waste of security forces' resources and lead to policy fratricide, especially if the Indian Armed Forces over-militarized policy to combat grey-zone activities. China and Pakistan's grey zone threat is an existential and futuristic danger that is unlikely to be addressed amicably in the near future. Anticipating and preparing for future battles is where strategic insight is found. According to Russian scholar Gerismov, future wars would be 75 percent non-contact and 25 percent contact. Even in the 25% contact zone, outright conventional wars are improbable[2]. Arzan Tarapore, writing in Carnegie India, argues that the Indian Armed Forces' lack of emphasis on grey zone capabilities has forced political leadership to respond to such threats with an all-or-nothing decision with the use of military force: either start a major conventional war or abstain from any military action[3]. The country must acquire capabilities in non-traditional and irregular domains. This would not only reduce military spending, but it will also improve conflict resolution. In general terms, desired grey zone capacities can be widely grouped in each component of Comprehensive National Power, which will have a direct impact on our ability to resist any challenge in the grey zone. There is a need for a "whole-of-nation strategy" that incorporates all aspects of national power, including diplomacy, information, military, and economic power (DIME).

COUNTERING GREY ZONE THREATS DURING CONVENTIONAL OPERATIONS

For decades, India has been battling a hybrid war in J&K with no success. History shows that no proxy war or insurgency has ever been defeated solely through the use of military force anywhere in the world. A case in point is the French military's series of tactical and operational successes in Algeria, which failed to prevent France's strategic loss of Algeria. When confronted with hostile neighbors who have a proclivity for hybrid warfare, the government and the Indian Armed Forces must rethink their strategy before it's too late. Some of the facets that a plan to counter grey zone threats during a conventional conflict must account for are discussed below.

The Whole of Government Approach Because of the predominance of non-military means, grey zone threats are distinguished from all other forms of conflict. According to Wither, "a reaction to a genuine threat of hybrid warfare would necessitate a thorough or whole-of-government endeavour, as non-conventional techniques of warfare cannot be resolved solely by military means[4]. To ensure synergy between all parts of government involved, structures and processes must be established through legislation with appropriate authority and responsibility.

Remove Vulnerabilities and Build Resilience It is critical that the current government addresses the root causes of social discontent and increases its delivery mechanism for resolving complaints from all walks of life. Ultimately, it is the adversary's ability to exploit cultural fault lines and vulnerabilities that is at risk. The term "resilience" refers to the ability to reduce one's vulnerabilities. Resilience also adds to deterrence in a hybrid context by minimizing the potential gains any attacker may hope to reap, as doing so makes it less likely that hybrid attackers will succeed in achieving their goals.

Bridge the Technological Gap To successfully counter hybrid threats, India must invest heavily in technical growth. Artificial intelligence, drones, big data, information technology, space, electronic warfare, autonomous weapon systems, swarm technology, cyberspace, biotechnology, and quantum technology are only a few examples of technologies that need to be vigorously absorbed and upgraded. In the hybrid domain, whoever has and uses futuristic technology creatively will have the upper hand.

Conventional Deterrence With unsettled boundaries, the threat of a conventional war looms large in the Indian context, and a loss of reliable conventional deterrence will result in substantial military embarrassment. As a result, India must strengthen

[2] https://jamestown.org/program/gerasimov-outlines-russian-general-staffs-perspectives-on-future-warfare accessed on 25 February 2021

[3] https://striveindia.in/shades-of-grey-warfare-options-for-india accessed on 25 February 2021.

[4] https://www.jstor.org/stable/26326441, by James K. Wither accessed on 25 February 21.

its military in order to maintain conventional deterrence against its enemies. Neglecting traditional capabilities, on the other hand, will empower non-state actors. State-sponsored hybrid war is intended to avert conventional warfare on a strategic level. It aims for perceived red lines and works underneath them. As a result, reliable deterrence may be the key to averting hybrid conflict.

Doctrine and Training From the unit to the army level, doctrine is the guiding thought that chooses actions. The doctrine should be written in basic, straightforward language and should be relevant to domestic circumstances and capacities. In the case of Israel, 'imported ideas' in the Israel Defence Forces (IDF) doctrine were referred to as a 'intellectual virus,' and were criticized for failing to withstand combat conditions during the Second Lebanon WarIndia faces a variety of threats; as a result, Indian military doctrines must address the full range of conflict and guide practical training and operational planning. In light of the Revolution in Military Affairs caused by the infusion of advanced technologies and hybrid means employed by the enemy, it is also necessary to reconsider the method of warfighting.

Proficiency in Combined Arms and Joint Fighting The armed forces must keep their combined arms and joint services operations skills up to date. The second Lebanon war's outcome was seriously hampered by a lack of understanding of combined arms operations, while Russia's fast combined arms operations in Ukraine and Crimea ensured quick success. It is high time for the Indian Armed Forces to advance to joint theatre command, where they will be able to provide joint structures down to the brigade level and perform more tactical joint services exercises.

Information Operations (IO) In the twenty-first century, information activities have emerged as the new center of gravity of modern wars. Information warfare, which encompasses psychological operations, cyberspace, and electronic warfare, has progressed from force multipliers to significant determinants of victory and defeat. India still has a long way to go in terms of technology and doctrine before it can successfully use IO as a war-winning factor; until then, it remains a major weakness. It is critical to develop skills in cyber operations, strategic communication, social media exploitation, and psychological operations. As the Islamic States (IS) and Hezbollah have shown, IO innovation is not solely dependent on technical advancement. Both used the United States' free Internet and media platforms to efficiently target the United States and its allies.

Structures and Institutions India is waiting for the military reforms to integrate the three services, as well as, changes within the government to integrate the military with the Ministry of Defence. The absence of dialogue between the political leadership and the military is unique to India and has been widely commented upon as a critical vulnerability. The government's appointment of the Chief of Defence Staff is a step in the right direction, but it must be accompanied by joint forces structures at all levels, from tactical to strategic, as well as a straightforward charter of responsibilities that includes command of all military activities. The reforms must be implemented as a whole rather than in pieces.

Develop Hybrid Capabilities Certain key military capabilities are required for hybrid conflict. These capabilities, such as Special Forces, mobile and agile units, trustworthy and real-time intelligence, mobile long-range artillery, drones, and so on, must be upgraded, and capabilities established against grey zone aggressors. India should conduct a net assessment of its adversary's potential vulnerabilities on a regular basis. The growth of hybrid capabilities and an information base in the grey zone would serve as a powerful deterrent.

CONCLUSION

In the twenty-first century, unrestricted wars in the grey zone are the most common form of conflict. This kind of war has raged between India and Pakistan for more than half a century, with no clear winner. As China adopts an aggressive position along India's borders and in the Indian Ocean region, the geopolitical situation in the region may become even more fragile. To counter the impending grey zone threats, India needs to take a proactive approach to developing capabilities and a cohesive national strategy. During a traditional war, grey zone threats will not erupt quickly; rather, they will be the result of the adversary's long-planned and well-thought-out approach, which will complement the aggressor's kinetic activities. As a result, we must develop new solutions for both offense and defence in the grey zone. While we prepare for the upcoming wars based on various circumstances, deeper synergy between several components of the country's political, military, economic, and information infrastructure will be required to achieve our National Security Objectives in near real - time, including countering the threat in the grey zone through an institutionalized whole-of-nation strategy.