



Hybrid Warfare Challenges to the Indian Defence Forces



Brigadier Mahipal Singh Rathore, VSM was commissioned into 17 JAK RIF and had the unique distinction of commanding 19 JAK RIF in Obstacle Ridden Terrain, Counter Terror environment, High Altitude Areas, Deserts & Amphibious Operations. He has been the General Staff Officer of an Infantry Brigade and Director of Perspective Planning (Strategic Section). He has been instructor at the Indian Military Academy, National Defence Academy and Army War College. He is presently commanding a Sector of the Rashtriya Rifles.

*“Future conflicts will be more violent and unpredictable with battlefields being severely contested and seamlessly connected. In future, even conventional conflicts are likely to have a large asymmetric component leading to hybrid war. Technology has become a key driver of future wars”.*¹

—General Bipin Rawat

Chief of Defence Staff (CDS)

Introduction

Hybrid Warfare covers the full spectrum of warfare by combining the vigour/ lethality of conventional warfare with the fervor of irregular warfare combined with the spectrum of technology for cyber and Information Warfare (IW). It also entails creating acts of criminal, legal and public disorder in the target country during peace time. Hybrid Warfare is hybrid not only in its ‘capabilities’ and ‘effects’, but, also in its ‘theory’ and ‘logic’. The aim of the paper is to define India's futuristic hybrid challenges and recommend ways to counter them.

Key Points

- Pakistan has been a master in Hybrid Warfare and its Proxy War in Jammu & Kashmir has been a success story.
- China specialises in 'Grey Zone' strategies & has been 'winning wars without fighting' to meet its global aspirations.
- Indian Defence Forces and security apparatus needs to build experts, systems and doctrines in multiple domains to win future hybrid challenges.

Pakistan has been a master at this game, ever since its independence in 1947, its prime focus has been on India. On the other hand, China has a strategic culture and is developing its military capabilities as per requirements of fighting a hybrid war. Therefore, future threats to India will be hybrid in nature which would include irregular tactics, terrorist acts and acts of criminal disorder including in the cyber domain. Likely aim of India's adversaries is to destabilise India by employing varied threats which are likely to manifest predominantly during peacetime and intensify during war in conjunction with employment of conventional forces. India's neighbours, particularly Pakistan has launched a sustained proxy war since independence and have used terrorism as an instrument of state policy against India in particular². Therefore, there is a need to look at these challenges and identify futuristic options that characterise a proactive approach for imposing caution on adversaries and thwarting their evil designs.

India's Strategic Orientation

India has primarily been a peace loving country that does not have an expansionist agenda. It strongly believes in living in 'peace and harmony; with its neighbours. Non-alignment and non-interference in the internal affairs of other countries has been a tenet of Indian's foreign policy notwithstanding brief interludes of liberation of Bangladesh (1971) and the Indian Peace Keeping-Force (IPKF) in Sri Lanka (1987-90). Well-being and development of its people, through sustained economic growth has been India's core national interest. However, a 'defensive mindset' over a long period, has modelled India into being a 'reactive power' and its responses have been situational and episodic³. The world at large considered India to be a soft state that did not respond resolutely even to the Proxy War unleashed by Pakistan till the recent Post-Uri Surgical Strikes (2016) and Post-Pulwama Balakot strikes (2019), thus showcasing a new resolve.

Exploitation of Hybrid Warfare by Pakistan

Pakistan has been, from time to time, using the 'tool' of hybrid warfare against India.

Pakistan's Strategy

The experience gained by Pakistan in equipping, training and providing leadership to the 'mujahideen' against the Soviets in Afghanistan was fully exploited in prosecuting a proxy war in J&K from the late 1980s. Pakistan abetted the insurgency in J&K in terms of training, equipping, leadership, financing and motivation. The overall aim of all elements operating, at the behest of Pakistan was common i.e. accession of J&K to Pakistan. An intense IW campaign was launched to spread fake news and propaganda, suppression of populace,

exploitation of anti-governance sentiments and fuelling of separatist sentiments in Kashmir. Pakistan irregulars, trained, equipped and led by regulars infiltrated periodically and locals were motivated to carry out acts of terrorism and create social disorder. These acts of violence resulted in the expulsion of minority 'Kashmiri Pandits' community, which changed the demographic profile in the Valley, which was part of Pakistan's overall strategy for a possible United Nations (UN) plebiscite in Kashmir.

*“In a new era of great power competition, our nations adversaries seek to achieve their strategic aims, short of conflict, by the use of layered stand-off in the political, military & economic realms.....”*⁴

—General Stephen J Townsend
US Army Training & Doctrine Command

Current Trends in Kashmir Valley

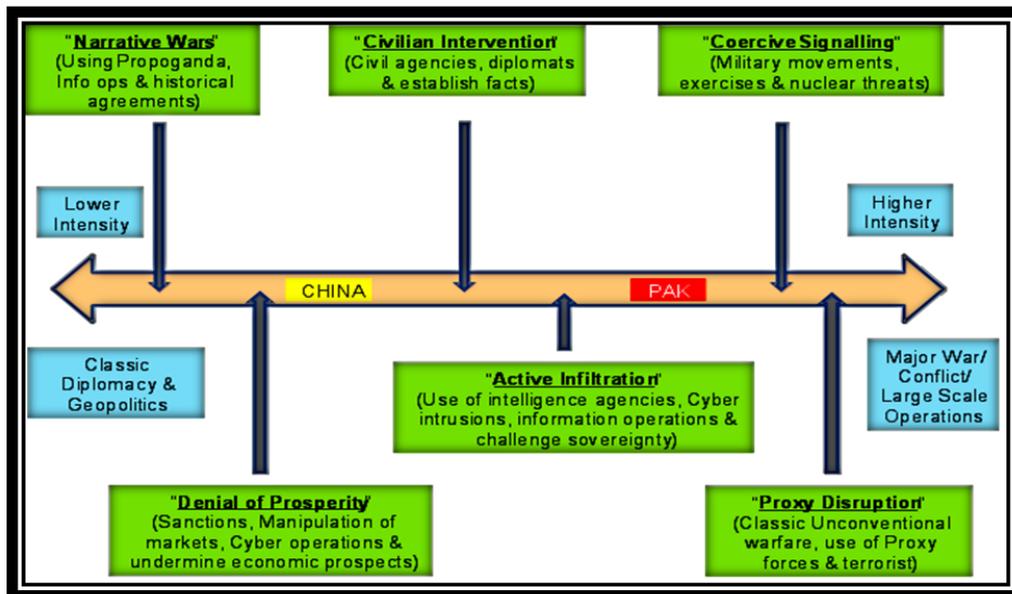
Post 2010 and more so after the Burhan Wani episode in 2016, agitational dynamics and radicalisation of the youth showcased the dangerous trends engineered by Pakistan using Social Media and Cyber space. However, the conflict now is shifting to both sides seeking domination of the 'mind space' of the population. This 'mind space' has been manipulated by inimical elements supported by Pakistan in the name of religion, ethnicity and distorted historical facts. Though contained in 2019 and 2020, after the FATF 'grey listing', the external involvement of Pakistan is likely to continue. Role played by Pakistan in fomenting violence in the Valley in the aftermath of Burhan Wani's death⁵ in 2016 is the most recent example of “grandiose design” of its proxy war⁶ by exploiting all components of Hybrid warfare.

Adoption of 'Grey Zone' Strategies by China

'Grey Zone' Warfare with Chinese Characteristics. China's use of gradual, multi-instrument strategy to amass a decisive legal foundation for its claims in South China Sea and more recently in North Sikkim, Pangang Tso and Galwan are clearly reflective of their 'Grey Zone' strategy. The various concepts that China adopts are 'Salami Slicing', 'Fait accompli' and 'Strategic gradualism'⁷, which becomes difficult for nations to comprehend as all these concepts are vague, and inconclusive lines to be able to differentiate one from the other. The Chinese national orientation towards Sun Tzu makes them ideally suited for unrestricted warfare including political, economic, resources and three warfares⁸. China's strength includes its synergised politico-military hierarchy, economic and diplomatic strengths and advances in high technology. China is likely to adopt a mix strategy of unrestricted warfare exploiting a large grey zone with a focus on non-contact and psychological warfare to avoid acts of direct confrontation against India. In this endeavor, its

reliance would be greater on technology and economy than in the human dimensions. Collusivity between Pakistan and China to compliment each other's capability is likely and China may provide Pakistan cyber and space warfare capabilities while enjoying a degree of deniability. This becomes all the more important as, during the visit of Chinese Defence Minister to Pakistan in November 2020, an Memorandum of Undertaking (MoU) for enhancing defence cooperation was signed.⁹ Pakistan would supplement Chinese efforts by putting its vast human intelligence network at its disposal. Unrestricted warfare by China is likely to take place in a time continuum with no clearly demarcated stages or phases as they are focused on 'winning wars without fighting' by exploiting tools of 'Grey Zone' warfare to their advantages.

Figure 1: Spectrum of Hybrid Techniques



Source: Annotated by author

As can be deduced from the above figure (Fig. 1), the intensity of China is lower and less pronounced by means of narrative wars, denial of prosperity by making debt ridden economies, unassuming civil interventions and are more in the 'Grey Zone'. While Pakistani efforts are more pronounced and are higher in intensity by means of proxy war, cyber intrusions, military movements, missile tests and use of proxies.

Chinese Capabilities. China has put in place organisational structures, equipment and infrastructure to wage successful offensive 'grey zone' warfare. One of the strategy articulated by China is 'Unrestricted Warfare'¹⁰, which implies similar capabilities as fighting a

hybrid war. China is competing with the United States (US) as a World Power and possesses hybrid capabilities that are highly developed and effective. China has an integrated Cyber Network Operations (CNO) with other components of IW like electronic warfare, psychological operations, kinetic strikes, space warfare and deception in an unified framework. This concept integrates all elements of IW-electronic and non-electronic, offensive and defensive, under a single command authority of the PLASSF¹¹. China actively collaborates with and funds civil IT companies such as ZTE, Huawei and Datang to gain access to cutting-edge Western technology. It has also formed 'IW militias'¹² comprising of personnel skilled in high technology areas of computers. The 'IW militias' are fully integrated with PLASSF at the Integrated Theater Command and Combined Corps level. Therefore, by shrouding their operational preparedness in secrecy, China has caused unease/ suspicion of its intent in the sub-continent. Chinese have steadily developed their space capabilities and integrated space-based electronic network of satellites with weapons and C⁴I²SR components that enables the launch of long distance precision attacks on the ground, sea or in space. Increased Indian dependency on Chinese companies in the digital domain has further enhanced vulnerabilities towards the Chinese cyber, information and psychological domains.

Economic and Resources Warfare. China is the second biggest economy in the world with a sustained growth rate of over six per cent. It possesses substantial economic warfare capabilities including blockades, blacklisting, preclusive purchasing and capturing enemy economic assets¹³. The huge trade deficit (\$ 54 billion) that exists between India and China provides considerable leverage to China to unleash an economic war against India.

Diplomatic Efforts in the Sub-Continent. China is developing neighbourly relations by following the 'debt trap' diplomacy¹⁴ and enhancing defence cooperation and infrastructure development projects in the Indian Sub-Continent¹⁵. Development activities at Gwadar, Hambantota, Coco Islands and in Nepal are some areas of concern. It aims to keep India entangled in solving the issues with its immediate neighbourhood.

Recommendations to Combat the Military Strategic Challenges

Below Threshold Operations. Indian Military planners will have to devise a strategy wherein, success would depend on creating more options below the threshold of conventional conflicts and kinetic operations along the disputed borders. New set of military engagements in the kinetic and non-kinetic domains would have to be identified and executed¹⁶.

Cross Domain & Inter Agencies/Services Integration. Efforts should be coordinated to achieve effects greater than the sum of its parts by looking at them holistically. Therefore, there is a need for developing cross domain and inter agency/service collaboration. For instance, all intelligence agencies dealing with China or Pakistan should have a subject matter expert for coordinating and integrating existing organised verticals, as operating in silo's is no longer an option.

Lack of Mandate. An essential prerequisite to counter Hybrid Warfare, especially the IW part, is capability building to launch CNO. Presently, the Indian Armed Forces lacks a clear mandate to acquire these capabilities, even in low technology domains like interception of GSM communication at tactical level in counter insurgency operations, whereas, the local police have made provisions to do the same. To achieve seamless flow of mobile and network interception inputs, it is important that the Armed Forces, operating in the UT of J&K, are given unhindered mandate for interception of technology based systems that the terrorists and their support systems are using.

Asymmetry with China. There is gross qualitative and quantitative asymmetric difference in the information domain between China's PLASSF and India's Defence Cyber Agency. We need to integrate all elements of information like space, cyber, IW & EW into one Command & Control structure to be able to counter the threat from our Northern adversary.

Military Planning. Indian Military planners have invested on resources for the development of conventional operation capabilities, without actually focusing on the capacity to build response forces for hybrid threats. The efforts required in the immediate time frame, if not addressed soon, will be of advantage to the adversary. Therefore, there is a need for 'hybrid-specific' equipments, organisations and systems, to be put in vulnerable places.

Fear of Escalation. The risk of escalation remains and Indian Armed Forces have for a long time believed in Pakistan's 'irrationality' and possibilities of a 'non-affordable' conflict, thus creating inadequate military response options against Pakistan. Hybrid warfare further complicates the process and raises ambiguities as the 'intent' of the adversary is questionable, vague and deniable. Indian military planners should keep enhancing India's conventional and response capabilities thereby, maintaining escalatory controls at various stages as part of hybrid or political-military coercion strategy.

Lack of Decisive Results. Hybrid warfare does not provide decisive results and therefore maintaining a status-quo seems like a viable option. The Indian administration should now

take steps to integrate Kashmiri's with the nation and build on the gains achieved post abrogation of Articles 370 & 35A.

Countering Adversial Challenges

Some of the ways to counter the hybrid challenges posed to India are as follows.

Against Pakistan. India's muscular foreign policy, surgical strikes and Balakot strikes have set a new normal in our response to Pakistan's Proxy war. There is a need to up the ante, by enhancing the capabilities for offensive hybrid warfare along the Western Borders to create deterrence in the sub conventional domain. This shift from 'only defensive' approach will assist in achieving the capacity to firmly counter all designs against India's unity, sovereignty and territorial integrity¹⁷. Therefore, the desired end state of the peace time campaign against Pakistan should focus on developing an offensive hybrid warfare capability and exploit the existing fault lines within Pakistan and countering their IW campaign in J&K. During a conflict, India's own Hybrid warfare elements can be unleashed to create a rear area security challenges for the Pakistan Armed Forces.

Against China. The strategy against China will have to be radically different as there is a need to evolve/strengthen India's own conventional capabilities and infrastructure without raising any alarm. The asymmetry that currently exists in the military, technology and economic domains can be offset to a large extent by launching hybrid warfare campaigns. Therefore, we must generate long-term options in the hybrid domain keeping present geo-strategic realities and sensitivities in mind. In case of a conventional conflict, these hybrid capabilities will play a crucial role in tilting the scale in India's favour.

Institutional Changes at National Level

Top Down Approach. The 'top down' approach emanating from the National Security Strategy is the traditional/preferred route¹⁸. In the absence of this strategy, clear directions must flow from the Cabinet Committee on Security (CCS) through the National Security Advisor (NSA) for planning and thereafter executing of hybrid campaigns. The various organisations and ministries as part of this approach can be divided into two levels i.e. primary level (CAB Sectt, MoD & MEA) and the secondary level (MHA, MoF etc). While most of the organisations do exist, however, some might have to be created/ mandated to launch offensive hybrid campaigns against adversaries.

Strengthening the Legal Provisions. China and Pakistan have been exploiting legal agreements of the British Era and India's internal constitutional provisions for waging Hybrid

warfare against us. For instance, Pakistan continuously refers to the abrogation of Article 370 as infringement of their sovereignty. Therefore, there is a need to formulate/amend these constitutional provisions and review past agreements /provisions through consensus and mutual agreements.

Unified Control Centre. Hybrid warfare campaigns must be planned and executed through a specialised Unified Control Centre (UCC) by integrating all the stakeholders (multi-agency approach) into one dynamic command and control centre. This centre should coordinate its efforts with the support of the National Security Council Secretariat (NSCS) for allocation of on a case-to-case basis, for various themes and from various organisations.

Changes at Services Level

Integrated Approach. Integrated Approach is a natural sequel to the 'whole of government approach'. The ideal model must involve the Chief of Defence Staff (CDS) as a single point contact/advisor to the CCS through the Defence Minister. Directions received through CCS should ideally be coordinated by the CDS through Headquarters - Integrated Defence Staff (IDS). A Special Forces Command (SFC) is ideally required for synergising assets/resources of all the three Services and for planning/ execution of offensive Sub conventional operations in the kinetic domain. However, till such time these ideal structures are created, we need to utilise the existing structures; with the Tri Services philosophy of "unity of effort". The newly created Tri-Services Special Operations Directorate¹⁹ would be ideally suited for designating it as the Nodal Agency for executing hybrid campaigns in the kinetic domain (mandated to the military for execution). There is also a need to upgrade the Defence Cyber Agency to a fully functional Cyber or Information Command.

Build Systems, Concepts and Doctrines for Multi-Domain Operations. Indian Armed Forces need to build concepts for operating in 'hybrid' as well as 'grey zones'. Since, most of the 'grey zone' campaigns are predominantly non-military in nature, therefore, there is a need to have concepts developed by integrating military experts, civilians in other instruments of power and scholars to build systems and doctrines for the future in the multiple domains of political, economics, space, cyber, sea, land and air to be able to compete and win future hybrid challenges from our adversary's to the North and West.

Theatre Level Changes. There is a need for creating Units at the Theatre and Operational level with a mix of dedicated IW Corps and General Staff personnel. Defence forces need to be given clear mandate to develop and deploy IW capabilities in counter insurgency/terror operating areas. Dependence on state police for technical intelligence should be replaced

with enhanced capabilities with Signal and Military Intelligence units developing high end cyber capabilities.

Conclusion

Hybrid warfare is a reality and we as a nation must accept and equip ourselves with futuristic capabilities. Military leaders should create futuristic assets towards creating suitable organisational and structural changes for executing the same. Indian military decision makers need to introspect, analyse and formulate concepts, doctrines and strategy to have an effective mechanism to deal with the ever growing reality of hybrid warfare. Therefore, it is time to up the ante and prepare for the future battles on a more advanced scale.

End Notes

¹ Outlook Web Bureau, “Future Conflicts will be more Violent, Unpredictable” Outlook, 13 July 2019. Available at <https://www.outlookindia.com/website/story/india-news-future-conflicts-will-be-more-violent-unpredictable-says-army-chief-general-bipin-rawat/334120>. Accessed on 12 Oct 2020.

²Narender Kumar, "War Beyond Rules:- “Hybrid War and India's Preparedness”, *CLAWS Journal* (Summer 2017). Accessed on 12 Oct 2020.

³James R Holmes, “India has a strategic Culture”, *The Diplomat*, 19 April 2013. Available at <https://thediplomat.com/2013/04/india-has-a-strategic-culture/>. Accessed on 13 Oct 2020.

⁴The US Army in Multi-Domain Operations 2028, *TRADOC Pamphlet* 525-3-1, 06 December 2018. Available at <https://adminpubs.tradoc.army.mil/pamphlets.html>. Accessed on 12 Oct 20.

⁵Abdul Hameed Khan, “Changed Security Situation in Jammu & Kashmir: The Road Ahead”, *IDSA Monograph Series*, Issue No 61, May 2017. Available at <https://idsa.in/system/files/monograph/monograph61.pdf>. Accessed on 20 Oct 2020.

⁶Parjanya Bhatt, “Burhan’s Shadow looms large in Kashmir”, *Observer Research Foundation*, 24 May 2019 Available at <https://www.orfonline.org/expert-speak/burhans-shadow-looms-large-in-kashmir-51178/>. Accessed on 20 Oct 2020.

⁷Michael J Mazarr, “Mastering the Gray Zone: Understanding a Changing Era of Conflict”, *United States Army War College Press*, December 2015, pp 79-101. Available at <https://publications.armywarcollege.edu/pubs/2372.pdf>. Accessed on 21 Oct 2020.

⁸Peter Mattis, “China’s ‘Three Warfares’ in Perspective”, *War on the Rocks (Special Series – Ministry of Truth)*, 30 January 2018. Available at <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>. Accessed on 21 Oct 2020.

⁹PTI, “China's Defence Minister meets Pak Army Chief ; Discusses Regional Security Issues”, *india.com*, 30 November 2020. Available at <https://www.india.com/news/world/chinas-defence-minister-meets-pak-army-chief-discusses-regional-security-issues-4234027/>. Accessed on 21 Oct 2020.

¹⁰Qiao Liang and Wang Xiangsui, *Unrestricted Warfare : China’s Master plan to Destroy America*. Originally published by PLA literature and Arts Publishing House, February 1999. Accessed on 12 Oct 2020.

¹¹Kevin L Pollpeter, Michael S Chase and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, *RAND Corporation*, 2017. Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR_2058/RAND_RR2058.pdf. Accessed on 12 Oct 2020.



¹²Kieran Richard Green, "People's War in Cyberspace : using China's Civilian Economy in the Information Domain, *Military Cyber Affairs*, Vol 2, Issue 1, Article 5 (2016). Available at <https://www.doi.org/http://doi.org/10.5038/2378-0789.2.1.1022>, available at <https://scholarcommons.usf.edu/mca/vol2/iss1/5/>. Accessed on 21 Oct 2020

¹³Major John A Van Messal, "Unrestricted Warfare : A Chinese Doctrine for Future Warfare", *USMC*. Available at <https://apps.dtic.mil/sti/citations/ADA509132>. Accessed on 21 Oct 2020.

¹⁴The 'New Great Game': China's Debt- Trap Diplomacy, *European foundation for South Asian Studies (EFSAS)*, October 2017. Available at <https://www.efsas.org/publications/study-papers/the-new-great-game-chinas-debt-trap-diplomacy/>. Accessed on 21 Oct 2020.

¹⁵Nilanthan Niruthan, "How Hybrid Warfare Could Change Asia", *The Diplomat*, 25 June 2016. Available at <https://thediplomat.com/2016/06/how-hybrid-warfare-could-change-asia/>. Accessed on 21 Oct 2020.

¹⁶Frank G Hoffman, "Hybrid Warfare and Challenges", *Small Wars Journal*. Issue 52, 2009. Available at <https://smallwarsjournal.com/documents/jfqhoffman.pdf>. Accessed on 21 Oct 2020.

¹⁷Anil Gupta, 'Is India prepared to Deal with Hybrid War?', *South Asia Monitor*, 08 December 2016. Available at <https://southasiamonitor.org/>. Accessed on 03 Dec 2020.

¹⁸Vikrant Deshpande, *Hybrid Warfare : The Changing Character of Conflict* (New Delhi: Pentagon Press, 2018). Accessed on 21 Oct 2020.

¹⁹Rajat Pandit, "Unified Tri-Service Agencies to handle Cyberspace, Space , Special Ops", *Times of India*, 25 September 2018, Available at <https://timesofindia.indiatimes.com/india/unified-tri-service-command-to-handle-cyberspace-space-special-operations/articleshow/65941584.cms>. Accessed on 21 Oct 2020.

The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.



CENTRE FOR LAND WARFARE STUDIES (CLAWS)

RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010

Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: landwarfare@gmail.com

Website: www.claws.in