Editorial

Dear Readers,

The targeted killing of two Iranians in two different ways in 2020 has once again brought to fore the unlimited ways in which Grey Zone war can be prosecuted. Major General Qassem Soleimani, the Iranian Revolutionary Guards commander, was killed in a US drone strike at Baghdad International Airport on 03 Jan 2020. Prominent Iranian scientist Mohsen Fakhrizadeh was killed in an attack outside Tehran on 27 Nov 2020. He was widely seen outside the country as a leading figure in the Islamic Republic's nuclear programme. The first killing was obviously in the Grey Zone. A state killed the national of another state in a third state, it also declared it had done so — using loopholes in international law to justify it. The second killing of Mohsen Fakhrizadeh was covert. His car was ambushed by unknown persons in a classic Grey Zone strike.

Grey Zone war is such an amorphous concept that there are varying definitions for it and strategic analysts have varying perceptions about it. In some cases, it is likened to simply unconventional war, while in other cases many other manners of harming the people and interests of a state are taken under its fold. This issue of the USI Journal is themed for Grey Zone war. The 11 articles herein attempt to throw light on it from varying angles.

In the lead article titled 'Finding the Way for India in the Shades of Grey: Capacious, Shadier, Murkier & Below the Belt', Lieutenant General Dushyant Singh, PVSM, AVSM (Retd) argues that in view of increasing grey zone conflicts against India, the national security strategy needs a paradigm shift in perspective that focuses on Conflict Prevention, Conflict Management, and Conflict Termination. This is followed by an article by Lieutenant General Ghanshyam Singh Katoch, PVSM, AVSM, VSM (Retd). He in the article 'Milestones on a Murky Road: Getting to Grips with the Grey Zone' says that understanding war in the grey zone is the first step to being able to face adversaries, for whom this is increasingly the only way of war.

The next is the article ‘Airpower in the Grey Zone’ in which, Air Marshal Anil Khosla, PVSM, AVSM, VM (Retd) brings out that Airpower can play a major role and can effectively be utilised in many ways in grey zone operations with a change in mind-set, organisational adaptation and some amount of capability enhancement, reorientation, and training. This is followed by an article titled ‘Dragon in the Misty Land, Chinese Influence in the North-Eastern Region: A Critical Analysis’ by Major General Vijay Ranade. The author highlights the fault lines in NE based on ethnic divergence, porosity of the borders and developmental deficit; these vulnerabilities can be exploited by grey zone actions.

The next article ‘The Determinants of India’s National Military Strategy’ is an abstract of the USI National Security Paper 2020 by Lieutenant General (Dr) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd). In the article titled ‘War: Yesterday, Today and Tomorrow’, the author Brigadier Manoj Mohan brings out the advancements in military relevant technology and connects it with the way war is presently planned to be fought.

For the next article, ‘Deciphering Grey-Zone Operations in Maritime-Asia’ by Commander Abhijit Singh (Retd), we thank the Observer Research Foundation (ORF) for their permission to carry this article, which was published as an ORF Special Report on 03 Aug 2018, in our Journal. This is followed by an article by Ms Poornima Balasubramanium. She in her article, ‘Securing India’s National Security in the Era of Grey-Zone Conflicts: Case of Cyber Warfare’ assesses the kind and level of threat posed by cyber-centric grey zone conflicts to Indian national security and international stability.

This is followed by an article titled ‘The Corona Whodunit: Grotesque from the Grey Zone’ by Group Captain (Dr) K Ganesh (Retd), wherein he comments upon many theories abound about SARS-CoV-2 being the by-product of Chinese experiments to produce a weapon with devastating effects and deniability for use in Grey Zone war. Wing Commander UC Jha (Retd) in the next article, ‘Grey Zone Conflict and Legal Derision’ highlights an urgent need to upgrade international legal frameworks and

mechanisms of conflict management which could be employed to address the Grey Zone conflicts.

The last article, 'Unconventional Warfare' by Major BN Sharma, appeared in the USI Journal in 1966 and is added to enable the reader to discern how the interpretation of this type of war has changed in the past 55 years. We would say that it has. The rest we will leave it to you to decide as you go through this issue of the USI Journal.

This issue also carries short reviews of the following books:

- Territorial Army: Gateway for Civilians to Army.
  By Lieutenant Colonel Surender Singh
  Reviewed by Shri Gaurav Kumar

- The Coolie's Great War: Indian Labour in a Global Conflict, 1914-1921.
  By Radhika Singha
  Reviewed by Sqn Ldr Rana TS Chhina, MBE (Retd)

As always, we await your valuable feedback and suggestions while we continue to maintain the standards of meaningful research and original writing.

Happy Reading!

The Editorial Team

Lt Gen Ghanshyam Singh Katoch, PVSM, AVSM, VSM (Retd)
Head Editorial Team

Gp Capt Sharad Tewari, VM (Retd)
Consultant Editor

Finding the Way for India in the Shades of Grey: Capacious, Shadier, Murkier & Below the Belt

Lieutenant General Dushyant Singh (Retd)[@]

"War in the 21st century is conducted at a roughly four-to-one ratio of non-military and traditional military tools and tactics".

—General Gerasimov,
Chief of General Staff, Russia

Abstract

In light of the progressively increasing grey zone conflicts against India, no instance of human error can be seen as unmotivated. Grey zone conflict has become popular in recent times because of its adaptability, cost-effectiveness, and relative lack of accountability. In such a scenario, the armed forces need to evolve and transform themselves to continue being a powerful protector of national security and ensure credible deterrence. Therefore, the national security strategy needs a paradigm shift in perspective that focuses on Conflict Prevention, Conflict Management, and Conflict Termination.

Introduction

It was a relatively quiet night in Mumbai on 12 October 2020, with the shadow of COVID-19 still looming large over it, when suddenly the economic capital of India and the 10th largest city in the world, with a population of over 1.2 crore, came to a grinding halt. Power was withdrawn from Mumbai for over two hours. All four grids that supply electricity to the city became non-functional

for two days, starting from 10 October 2020. Mumbai, the city of dreams for millions of Indians, the city that never sleeps, witnessed an unprecedented blackout seldom experienced by the *Mumbaikars* in the past few decades. Local trains, hospitals, water services, ticketing systems, everything was affected by the outage. Only after duration of two hours did some essential services were restored, that too in particularly critical areas of the city.

Is it surprising? Yes, because the city of Mumbai runs on an almost fail-proof electricity grid. Was this a grey zone war attack by China? Yes, it could be.[1] Such incidents are bound to increase in future given the factor of deniability and the low cost. The grey zone presents a broad canvas of options to warring countries to wage a war in the form of propaganda, misinformation, cyber-attacks, economic coercion, terror attacks, proxy war; the list and options are endless. The grey zone is used as an umbrella term to include hybrid warfare, proxy warfare, and non-contact warfare. Due to the inherent advantages of operating in the shades of grey, various nation-states are using it as a favoured tool to secure a strategic advantage in a geopolitical contest. While grey zone activities, such as covert operations to destabilise a country or to influence an election for a regime change, have been practised by countries in the past, the tsunami of technology due to the advent of expandable Artificial Intelligence (AI) and cyber, 5G, robotics, UAVs, space-based technologies have made it a preferred form of combat.

India has been a victim of grey zone tactics by Pakistan through the use of non-state actors for a long time now. The threat is increasingly becoming more sophisticated and formidable. There is a need to evolve a well thought-out strategy to deal with such threats against India. However, before we can do that, it would be imperative to understand this form of warfare so that the grey zone threats can be identified correctly and the policies, doctrines, and strategies to counter such threats can be evolved.

Making Sense of Grey Zone Warfare

Amidst various terms like the ‘Fourth Generation Warfare’ which is characterised by the involvement of non-state actors, ‘New Terrorism’ exemplified by the inhuman band of terrorists

envisioning the apocalypse, ‘Small Wars’ which is an American lexicon for Guerrilla Warfare and ‘Low Intensity Conflict’ which focuses on some level of violence with predominantly intra-state actors, it is the Hybrid Threat which has received the greatest traction in the current discourse. The term’s genesis is from American War Studies, premised on the realisation that since 9/11, the complexity of international conflicts has increased, with regard to the number and the kind of belligerents and tools adopted by the perpetrators. The related term ‘Grey Zone Warfare’ is often used interchangeably with Hybrid Warfare, but there remain pertinent differences between the two.

“Hybrid conflicts are full spectrum wars with both physical and conceptual dimensions: the former is a struggle against an armed enemy and the latter is a larger struggle for the control and support of the combat zone’s indigenous population, the home fronts of intervening nations, and of the international community. To support and stabilise the indigenous population, the intervening forces must immediately build or restore security, essential services, local government, self-defence forces and essential elements of the economy”.[2] On the other hand, grey zone conflict suggests “being in the metaphorical state between war and peace, where an aggressor aims to reap either political or territorial gains associated with overt military aggression without crossing the threshold of open warfare with the adversary”.[3] Mark Galeotti of the Institute of International Relations in Prague describes these approaches as “Guerrilla Geopolitics”.[4]

The US Department of Defense (DoD) defines the grey zone as, “a conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve politico-security objectives with activities that are ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale direct military conflict, and threaten nations and allied interests by challenging, undermining, or violating international customs, norms, or laws”.[5] David Carment, Dani Belo[6] and Hoffman[7] have defined grey zone along similar lines with minor variations. However, most of these definitions have a negative connotation. Andrew H. Cordesman has suggested that activities in the grey zone also have a positive overtone and serve to achieve a strategic advantage in

geopolitical competitions.[8] He has defined grey zone as, "Every activity that has an impact on achieving strategic advantage vis-à-vis your adversary in a strategic competition or conflict military or non-military and falls short of conventional war using positive, negative actions in multifarious domains will be considered as part of grey zone conflict".[9] Figure 1 refers to various domains of the Grey Zone.[10] This paper will use the broader definition for further classifying a grey zone activity. The ambiguity of grey zones is often exploited at multiple levels by nations to overcome international laws and create an ambiguous world order.

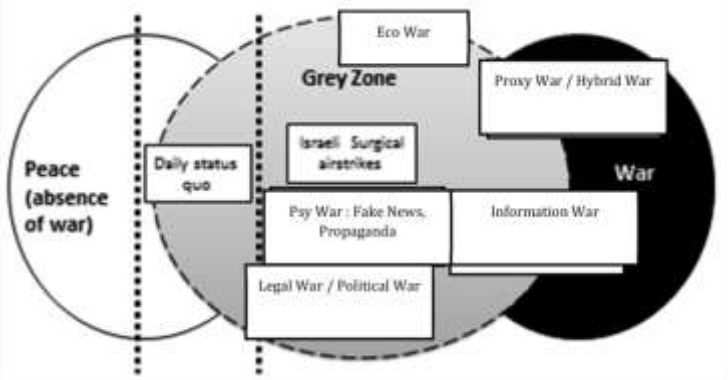


Figure 1: The Grey Zone

Why do Countries indulge in the Grey Activities over Conventional Conflicts?

Low economic and human costs vis-à-vis conventional wars motivate countries to indulge in grey zone conflicts. The US expenditure on wars in the Middle East and Asia since 2001 has approximately been USD 6.4 trillion. In the fiscal year of 2019, it was around USD 2 trillion.[11] The report by the Watson Institute of International and Public Affairs, Brown University concluded that more than 801,000 people have died due to fighting, and another 21 million people have been displaced.[12] For J&K conflict, between 1989 to 2004 Centre has reimbursed Rs 3101.87 crore to the state.[13] Against this, Pakistan has spent a minuscule amount, both in terms of human lives and funds. Likewise, the emergence

of disruptive technologies using expandable artificial intelligence, quantum computing and cyber technology have provided easy tools to wage such wars. The other reasons that motivate countries to use grey zone are the lack of deniability and responsibility.

Important instances of Grey Activities against India

The cyber-attack on the Mumbai power grid started from October 10, 2020 onwards. The first power grid that supplies electricity to Mumbai was shut on the day following a 'technical failure'. Two days later, the circuit of another transmission line tripped. That was followed soon after by another circuit line tripping, and this had a cascading effect on the Pune – Kharghar and Talegaon – Kharghar lines too. Mumbai power grid works on a unique Islanding principle which is 99 per cent fail-proof, set up as early as in 1981. Thanks to this system, the city has successfully negotiated 27 of the 37 major grid disturbances in the last four decades.[14] However, on 12 October even the Islanding system failed. The Mumbaikars pay an annual surcharge of Rs 500 crore to ensure the uninterrupted backup of power up to 500 Mega Watt (MW).[15]

What is more disturbing to note is that this occurred just a few months after the Galwan incident in Eastern Ladakh, in which 20 of our gallant soldiers were martyred due to an unprovoked action by the Peoples Liberations Army (PLA) of China. Was it an instance of sabotage by the Chinese Cyber Cells? If we go by the Cyber Cell of the Mumbai Police, it was possibly the result of a sophisticated sabotage attempt involving foreign entities. On the other hand, if we go by the statement of Mr RK Singh, Minister of State (Independent Charge) for Power, Government of India, the blackout was a result of human error. While the truth may not be immediately evident but the possibility of a cyber-attack on the power grid of Mumbai cannot be ruled out entirely if we are to believe the findings of the month-long probe by Mumbai Police Cyber Cell. Abhishek Sharan, quoting a reliable source, has stated that hackers have been trying to target the country's power utilities since February 2020.[16]

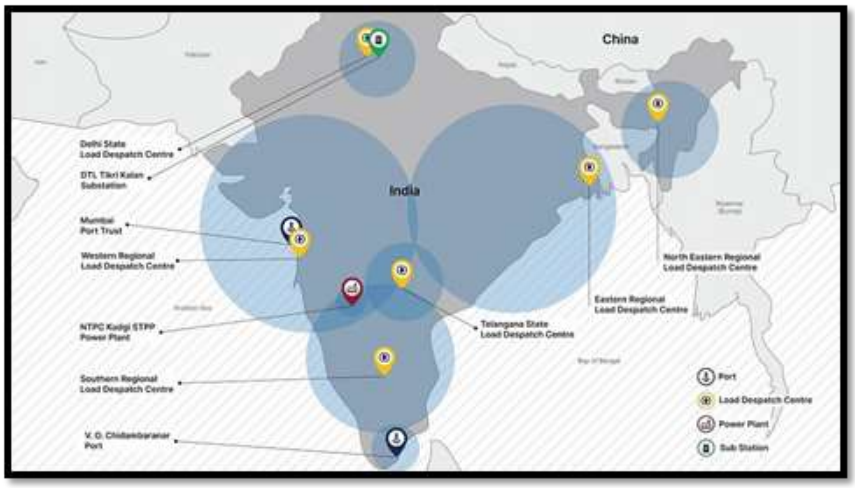
The cyber attack on the country's Power Grid by Chinese hackers once again grabbed headlines when 'Recorded Future's Insikt Group', a Massachusetts based cyber security firm, released a report on the details of the cyber-attacks on India. From mid-2020 onwards, Recorded Future's midpoint collection revealed a steep rise in the use of infrastructure tracked as AXIOMATIC ASYMPTOTE, which encompasses ShadowPad command and control (C2) servers, to target a large swathe of India's power sector. Ten distinct Indian power sector organisations, including 4 of the 5 Regional Load Despatch Centres (RLDC) responsible for the operation of the power grid through balancing electricity supply and demand, have been identified as targets in a concerted campaign against India's critical infrastructure (See Map 1). Other targets identified included two Indian seaports.[17] The pro Chinese hackers who are operating from many countries may just have proof-tested their systems. Therefore, their ability to damage, disturb or destroy our systems cannot be ruled out.

China has fought a war with India in 1962 and a localised war in 1967 at Nathu La. We lost the first one because of lack of preparedness but won decisively in the second. Having realised the futility of fighting a conventional war, it has used its military strength for deterrence and simultaneously waged a series of grey zone conflicts along our Northern borders. It has done this through face-off transgressions across the Line of Actual Control (LAC) in Ladakh, Sikkim and Arunachal Pradesh, especially in the last two decades. China is also leveraging its economic strength to bring down our economy. The recent example of China trying to swamp Indian economy through ASEAN sponsored Regional Comprehensive Economic Partnership (RCEP) is a case in point.[18] Similarly, its attempt to purchase shares in the HDFC Bank[19] followed by the border face-offs at multiple points[20] in Ladakh despite COVID-19 are other instances of a grey zone war.

Galwan was by far the most skillful grey zone activity of China. The Chinese miffed with India's stand on the spread of the Corona Virus and the abrogation of Article 370 and 35 A, the construction of the Leh - Darbuk - Shyok - DBO Road, decided to test the Indian resolve to defend its territory by carrying out minor

border confrontation in Naku La on 10 May 2020. Emboldened by our routine response, the PLA launched their operations to change the status quo in Eastern Ladakh in areas of Hot Springs, Gogara, Galwan and Pangang Tso.

India was misled into believing that the Chinese would honour their commitment of 06 June 2020. China instead resorted to unprovoked violence on 14 June 2020, on our unsuspecting troops in the Galwan Sector, while they were verifying on the ground whether the Chinese troops had vacated the areas where they had transgressed. Colonel Santosh Babu and 20 of our brave soldiers were martyred but not before they killed 30-35 Chinese soldiers. The two Asian powers are once again engaged in border military-to-military talks. If we reflect upon the course of events, it clearly emerges that the Chinese are at their old game of talk — talk and fight — fight. The deliberate avoidance of firearms was to keep the conflict below the threshold of a conventional war. This is an essential ingredient of grey zone conflict. The Chinese once again have played smart by achieving the withdrawal of Indian troops from the Kailash ranges, a feature that was providing observation into the Chinese activities. On the other hand, they continue to hold on to their positions in Hot Springs, Gogara and Dapsang plains. The military talks after the partial withdrawal of the two sides in Pangang Tso sector appear to be a tactic to fool us and strike again at an opportune time. Dean Cheng in "The Daily Signal" on US – China military engagements has written, "Mao would negotiate, not in order to "get to yes" and reach a compromise solution, but to buy time, colour his opponent's views, and influence third parties. The ultimate goal never changed whatever the negotiating position".[21] This quote is loaded with messages for India. China will spare no efforts to rest the LAC along Indus - Shyok Rivers, however, we need to prevent China from succeeding at any cost.



Map 1 : Regional Load Despatch Centres

Map 2: Conflict Areas between India and China

Grey threats from Pakistan and other countries/entities continue to inflict India since the last four decades. Pakistan, in particular, has been extremely active by waging a Proxy War, first in Punjab and now in J&K. Since 1994, over 60,000 lives have

been lost, of which over 40,000 are from J&K. Besides this, Pakistan also actively hacks into various governmental and non-governmental websites which cause a loss of business and a loss of intelligence. In addition, it has been conducting an information war by highlighting exaggerated human right violations in the J&K, distorting reports about the Indian security forces actions against rioters and protesters on issues such as National Register of Citizens (NRC) / Citizenship (Amendment) Act (CAA). It also hobnobs overtly with Hurriyat and other pro-Pak political parties to undermine India. There is also a common perception that most of the grey zone activities against India only emanate from China and Pakistan. However, this is far from the truth. There have been a number of instances of grey operations launched by friendly nations to promote their national interests. A case in point is the Dalit agitation in April 2018, which was believed to have been orchestrated by US-based Pro-Dalit Groups using AI, Big Data, and by purchasing social information from Social Media platforms and comparing them with Indian Census Data.[22] Similarly, the news articles that emerge from various foreign media houses on CAA, NRC, the Farmer's agitation, and now the COVID crisis betray the intention to undermine the country and its government. Such activities are also carried out with the tacit support of internal anti-social elements inimical to the ruling dispensation.

Recommended Approach

The grey zone threat from China and Pakistan is unlikely to be resolved amicably. Strategic wisdom lies in the anticipation of and preparation for future wars. To instil desired capabilities in India, there is a requirement for an in-depth study of several alternative future security environments. Comprehensive National Power (CNP) will directly bear on our ability to withstand any challenge in the grey zone. The recommended approach in various domains of CNP is, firstly, political and diplomatic dexterity to ensure fail-proof alliances while continuing to engage with China at the desired level, backed up by sound military diplomacy. Military diplomacy needs to be scaled up to project desirable military signals at the intended target audiences. Secondly, the information age has already stepped into new realities of machine learning, artificial intelligence, and robotics. The strong software base in India needs

to be supported by indigenous hardware design and production capability. Given the growth lag in this sector, India should collaborate with countries like Singapore and South Korea as an offset to trade negotiations. Related challenges of attracting and retaining talent for the national cause need to be dealt with comprehensively. Thirdly, the safety of our information infrastructure and critical data needs to be ensured by creating backup and reducing redundancy in communications, power transmission, aviation and railways. Cyber-attacks are a reality that needs refined, comprehensible, and easy-to-execute crisis management plans along with indigenous offensive capability to escalate cyber deterrence. Fourthly, the offensive Space capability needs to be developed on a priority basis. Any defensive architecture is prone to get breached unless the adversary is also conscious that his infrastructure and national systems can also be targeted significantly, if not comprehensively. Keeping Anti-satellite weapon (ASAT) capabilities as mere technology demonstrators will not be sufficient. Furthermore, cognitive susceptibilities of the armed forces personnel and people are areas of intangible gains for our adversaries. There is an urgent need for a strong internal communication mechanism to dispel rumours and misinformation. The potential flash-points have a propensity to turn into major public order situations and need to be kept under constant vigil while enhancing own Technical Intelligence (TECHINT) and Human Intelligence (HUMINT). These need to be integrated with national Intelligence, Surveillance, Reconnaissance (ISR) infrastructure to ensure common operating picture by all stake holders. Linguistic skills to include most spoken dialects of languages in regional states should be enhanced and harnessed, both by cyber agencies and the stake-holders engaged in any form of strategic communication. Offensive measures to spread similar vulnerabilities in the adversary must be integral to our efforts. Sixthly, economic decoupling from China is a fait accompli being our primary threat. We need to find alternate trading partners, and for this, we have to exploit the QUAD, friendly countries in the ASEAN, the Middle East (ME), Africa and the Americas. We also need to focus on self-reliance or the *Atmanirbhar Bharat* initiative. Seventhly, in military security, there is a need to create completely

integrated armed forces which are future-ready. Keeping the multi-domain nature of grey zone threats in mind, the transition to Integrated Theatre Command System has now become mandatory to respond effectively to threats. Most of the armies in the world have already transformed into integrated/joint structures. Cyber war, information war, out of area contingencies, and hybrid threats are some of the areas wherein the integration of resources is imperative. The agility in a force is induced by its readiness profile, mobility, and quick transformation from one role to another without major logistic liability. Future engagements like Galwan and Dokalam are likely to occur unanticipated and the response thereof has to be rapid and lethal. Therefore, agility and the ability to operate in an environment of information vacuum is the key to our success. Such threats can best be tackled through technically empowered and enabled Special Forces. Special Forces should also have the capability to operate beyond the Indian Territory. This is an imperative considering India's strategic interests, stakes in the Indian Ocean Region, and the widespread Indian diaspora. Let us not be shy of protecting our regional and extra-regional interests, if required, by the use of the military. Finally, a robust and rapid response mechanism should decide the success or failure of response to a grey zone threat given the long northern borders of our country and severely restricted border infrastructure. Our intelligence agencies should forewarn and prepare the security forces for the impending threats.

Conclusion

Contrary to the view of many Western academics and journalists, Gerasimov emphasises that there is no model or formula for warfare, but rather each scenario is markedly unique and requires a tailored approach.[23] Therefore, we need to evolve our own solutions both for offence and defence in the grey zone. There will be a requirement of greater synergy between all security architecture components, which needs to be dovetailed in our Foreign Policy Objectives in real time to meet the grey zone threat. To ensure a credible deterrence and responsive capability against emergent grey threats, there is a need to institutionalise the whole nation's approach to the national security matters. Thus, the national security strategy in the grey zone should constitute -

Conflict Prevention, Conflict Management, and Conflict Termination Strategy.

Endnotes

[1] Sahil Joshi, “Mega Mumbai power outage may be result of cyber attack, final report awaited”, *India Today,* Nov 20, 2020, https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20

[2] John J McCuen. “Hybrid Wars”. *Small War Journal, Military Review,* Mar-Apr 2008, Also cited in Dr. Russell W, Glenn. “Thoughts on Hybrid Conflict”, Small Wars Journal. Accessed on May 15, 2021. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_ art017.pdf .

[3] Abhijit Singh; “Between War and Peace: Grey Zone Operations in Asia”, *Australian Outlook,* Feb 2018. Accessed on May 15, 2021. https://www.internationalaffairs.org.au/australianoutlook/paramilitaries-grey-zone-operations-asia/ .

[4] Manea, Octavian. “Russia is Practicing a form of Geopolitical Guerrilla War against the West”, *Defence Matters,* December 2017. Accessed on May 12, 20121. https://www.defencematters.org/news/russia-is-practicing-a-form-of-geopolitical-guerilla-against-the-west/1320/ .

[5] George Popp and Sarah Canna. “The Characterisation and Conditions of the Grey Zone”, *Boston, Mass: NSI Inc, Winter 2016.* Accessed May 12, 2021. http://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf.

[6] David, Carment, and Dani Belo, *War’s Future: The Risks and Rewards of Grey - Zone Conflict and Hybrid Warfare. 2018.* Accessed May 14, 2021. https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare.

[7] Frank G. Hoffman, “Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges,” *National Defense University, (PRISM Volume 7 no. 4), November 8, 2018.* Accessed April 14, 2021. https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/. (As quoted by , “Andrew H. Cordesman. “Chronology of Possible Russian Gray Area and Hybrid Warfare Operations.” Centre for Strategic Studies and International Studies, Washington, Rhode Island. https://csis-website-

prod.s3.amazonaws.com/s3fs-public/publication/200702_Burke_Chair_Russian_Chronology.pdf . p. 8.

[8] Andrew H. Cordesman. “Chronology of Possible Russian Grey Area and Hybrid Warfare Operations.” *Centre for Strategic Studies and International Studies, Washington, Rhode Island.* Accessed April 14, 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200702_ Burke_Chair_Russian_Chronology.pdf . p.13.

[9] Ibid.

[10] Raik, Gilad. “The Diplomatic Manoeuvre.” *Belfer Center, RECANATI-KAPLAN FELLOW PAPER AUGUST 2016.* Concept adapted from the figure in the document mentioned in the paper. Accessed May 21, 2021. https://www.belfercenter.org/sites/default/files/files/publication/Diplomatic%20Maneuver%20-%20web.pdf .

[11] Macia, Amanda, “America has spent $6.4 trillion on wars in the Middle East and Asia since 2001, a new study says”, CNBCNov 20, 2019. Accessed May 21, 2021. https://www.cnbc.com/2019/11/20/us-spent-6point4-trillion-on-middle-east-wars-since-2001-study.html .

[12] Ibid

[13] Annual Report 2004-05. *MHA, Government of India.* Accessed May 21, 2021. https://www.mha.gov.in/sites/default/files/AnnualReport_04_05.pdf. P14.

[14] Karan, Pradhan . “How China-linked group RedEcho is targeting India’s power grid: The Recorded Future interview10:35:46 IST”, First Post, March 09, 2021. Accessed April 21, 2021. https://www.firstpost.com/india/how-china-linked-group-redecho-is-targeting-indias-power-grid-the-recorded-future-interview-9393741.html .

[15]Abhishek, Sharan. “40300-hacking-attempts-suspected-from-entities-in-china-to-cripple-utility-infra-services,” *Mumbai Mirror, Mar 1,* 2021. Accessed March 25, 2021. https://mumbaimirror.indiatimes.com/mumbai/crime/40300-hacking-attempts-suspected-from-entities-in-china-to-cripple-utility-infra-services/articleshow/76477568.cms .

[16] ibid.

[17] INSIKT GROUP, Feb 28, 2021, “China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions”, Recorded Future, Accessed March 25, 2021. https://www.recordedfuture.com/redecho-targeting-indian-power-sector/.

[18] ET Bureau. “India decides to opt out of RCEP, says key concerns not addressed”. Economic Times, 05 November 2019 . Accessed May 21, 2021. https://economictimes.indiatimes.com/news/economy/foreign-trade/india-decides-to-opt-out-of-rcep-says-key-concerns-not-addressed/articleshow/71896848.cms.

19 Rajesh Mascarenhas. *Economic Times,* April 13, 2020. Accessed May 24, 2021. https://economictimes.indiatimes.com/markets/stocks/news/chinas-central-bank-holds-1-stake-in-hdfc/articleshow/75104998.cms#:~:text=MUMBAI%3A%20China’s%20central%20bank%20has,India’s%20biggest%20housing%20mortgage%20lender.&text=The%20stock%20rallied%2014%20per,at%20Rs%201%2C702%20on%20Thursday.

[20] Indrani, Bagchi. “What’s behind Chinese intrusions? Beijing needs to save face globally. Expect a long LAC face-off and no solutions”. *The Times of India,* 4 June 2020, Accessed June 04, 2020. https://timesofindia.indiatimes.com/blogs/Globespotting/whats-behind-chinese-intrusions-beijing-needs-to-save-face-globally-expect-a-long-lac-faceoff-and-no-solutions-2/.

[21] Dean Cheng. ’Fight Fight, Talk Talk’: China’s Model for Military-to-Military Relations’. Daily Signal, July 27, 2011. Accessed May 24, 2021. https://www.dailysignal.com/2011/07/27/fight-fight-talk-talk-chinas-model-for-military-to-military-relations/ .

[22] PTI. “AI, GIS, big data helped in successful Bharat Bandh on April 2: Dalit activist”. *Economic Times, Apr 17, 2018.* Accessed May 24, 2021. https://economictimes.indiatimes.com/news/politics-and-nation/ai-gis-big-data-helped-in-successful-bharat-bandh-on-april-2-dalit-activist/articleshow/63799198.cms .

[23] David Carment and DaniBelo,”War’s Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare”, Canadian Global affairs Institute, October 2018. Accessed May 24, 2021. https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare.

@**Lieutenant General Dushyant Singh, PVSM, AVSM (Retd)** is an Infantry officer. He is an alumnus of the National Defence College, Defence Services Staff College, the College of Defence Management and the Naval Post Graduate School California, USA. He has served in the UN as a Military Observer. He also served in the elite National Security Guards as the DIG (Operations) and the IG (Operations). He has commanded a Corps and thereafter headed the Army War College.

Milestones on a Murky Road: Getting to Grips with the Grey Zone

Lieutenant General Ghanshyam Singh Katoch (Retd)[@]

Abstract

In terms of war, Grey Zone war is war waged in an indeterminate manner which is different from the commonly understood concept of war. Increasingly, in modern day war rules of a globalised world are bent to enable the war to be fought in a winnable manner. This is often done by a weaker side. However, over time it is also something being done by the stronger side to make war more economical, or to 'fight fire with fire'. Understanding war in the Grey Zone is the first step to being able to face adversaries for whom this is increasingly the only way of war.

Introduction

The 'Grey Zone' was a term coined by the Italian Holocaust survivor Primo Levi in his essay collection – *The Drowned and the Saved.*[1] It refers to an area of uncertainty, or indeterminacy, where there are no clear rules of conduct. The term 'black and white' refers to an issue having no ambiguities. Either a thing is good or bad; right or wrong. In other words, the polarity of the ends of a range are clearly defined and known. In polar opposites where the ends are black and white, then in between there will be 'shades of grey'. Traditionally white colour, especially in Christian tradition, signifies good, Jesus wears white clothes, angels have white wings, and white in context of daylight holds no terror or mystery because in light everything is visible. Black, on the other hand, signifies the unknown, terror and evil because primeval man at night could not view threats which could harm him. In terms of war, the Grey Zone lies between the two poles — war conducted

as per rules and war conducted without rules — between just war and unjust war.

The Milestones of the Changing Shape of Conflict

The requirement of having some rules and laws under which war should be conducted emerged consequent to the Geneva Convention of 1864 which was basically about the "Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field". It was only in the 1899 Hague Conference that codification of the laws of war on land as the "Hague Conventions 1899" was undertaken.[2] The wars post that convention used the rules that emerged to interpret the *'Jus in Bello'* concept or the 'Just way to wage war'. In a short period of less than a century since the laws emerged, countries and organisations had learnt to circumvent the rules.[3] The ways in which they circumvent the rules are such that nations or international multilateral organisations are not able to take legal action against those who break the rules.

Between 1648 (when the Treaties of Westphalia were signed) and 1949, written international laws gradually brought in rules to wage war. These included restrictions upon persons who were not uniformed members of armies from taking part in wars. If the people took up arms it was an insurrection. Those who did not wear uniforms or did not have a fixed distinctive emblem recognisable at a distance[4] and participated in war were treated as criminals (or terrorists) who could be killed without compunction. Conversely, those in uniform could expect quarter as per the laws of war.[5] Only the state had the right to use organised violence. However, we have also seen many examples of wars where uniforms are not worn — at least by one side. Where there is no formal hierarchical organisation, where at least one side operates within the population and does not adhere to the laws of war. These are wars in the Grey Zone.

As given above, in formal armies the soldier wears distinguishing marks on his uniform which identify him as a member of a particular state's army. However, in the Grey Zone this can be hidden. An example is the Little Green Men[6] in Ukraine who were clearly part of an army but denied being part of any state. By circumventing this distinction, they waged a sort of proxy war enabling a secessionist non-state to have an ally.

Another example is the Taliban, who while not being a state are a de facto state. So far, they have generally fought with undistinguishable clothing. The Taliban were a Grey organisation. The agreement signed between the Taliban and the United States at Doha on 29 Feb 2020 was a curious phenomenon. The most powerful country in the world signed a peace agreement with a non-state and in 16 places in the document referred to the entity with which they were concluding a peace agreement as "the Islamic Emirate of Afghanistan which is not recognised by the United States as a state and is known as the Taliban"![7] But a curious phenomenon which is now occurring is that to gain the legitimacy of a state, the Taliban army is morphing into a regular army with its elite troops wearing uniform/distinctive emblems.[8]

The Islamic State of Iraq and Syria (ISIS) is another manifestation of conflict in the Grey Zone. It is a terrorist militant organisation which unlike previous similar groups was a proto state. Its profound ambiguity is reflected in the confusion about its name in the media at a particular point of time when it was at its zenith[9] as well as the incomprehensible logic of whom is it fighting against. Is it other states, perceived apostates, colonial injustice, or perceived degenerate ways of life? Others indulging in violence in the Grey Zone are militarised drug cartels and organised crime syndicates. Lastly, a product of Grey Zone conflict is police forces worldwide which dress like and are armed like the army and armies which have to be empowered with police powers through special legislation to operate in the Grey Zone. It is obvious that Grey Zone challenges arise because of diverse reasons and do not throw out a single solution. How one state tackles it is not fully applicable to another because the factors which lead to conflict overlapping in the Grey Zone may be widely varying.

Operating in the Grey Zone

Grey Zone conflicts are not formal wars. If the spectrum of conflict ranges from peaceful interstate competition on the far left to nuclear war on the far right, Grey Zone conflicts fall left of centre.[10] They involve some aggression or use of force. Their primary hallmark is ambiguity — about the ultimate objectives, the participants, whether international treaties and norms have been

violated, and what tasks does the military take on to combat them.[11]

Responses to wars in the Grey Zone are increasingly being recognised as resting on political and police coordination and a coordinated interagency response. The military may not be the ideal instrument to head a Grey Zone war because such conflicts are designed, almost by definition, to circumvent traditional military power. Hence, they may take place within the population of a state and not necessarily on inter-state borders. Yet, military capabilities will remain an essential part of responses because success for the proponent of Grey Zone war is based upon being superior to the police forces. Police forces, therefore, need backing by military power. The other alternative is for them to get militarised. This is what is happening the world over. In a Grey Zone, boots on the ground are an essential component. Therefore, a larger force which combines the functions of the army and the police is best suited for this form of war. The French Gendarmerie and Italian Carabinieri exemplify this concept as they are military forces with police powers. So does the National Security Guard (NSG) of India, a premier federal counter terrorism force. It is a paramilitary force with 52 per cent military component on secondment for fixed tenures to the Ministry of Home Affairs. Control is with the police and cutting-edge counter-terrorism capabilities with the military.

When a conflict is intra state, to differentiate the adversary from among the population requires excellent intelligence. It would not be incorrect to state that the success of the police in the Punjab insurgency (1983-1993) was more the result of the intelligence they provided to the Police Commandos and the army than from their own militarisation. Indeed, state police forces are to that extent more important than the central or provincial armed police forces. They are the foundation on which the intelligence and security structure in intra state Grey Zone conflict must rest.

Nowadays, more states in the world are fighting non-state enemies than ever before. These enemies can be religious zealots (ISIS, Al Qaeda, Al Shabaab, Boko Haram etc.), separatists (various Pakistan sponsored groups in Kashmir, Chechens, Kurdish groups, Ukrainian groups etc.), those who want a change in the form of government (Taliban, Naxalites, Revolutionary Armed Forces of Colombia (FARC) etc.) or just criminal gangs (Mexican and South American drug cartels). While this is alien to mainstream conventional war, irregular warfare has been the proven way to fight a superior enemy. *Chhatrapati Shivaji* used it against the Mughals, the American revolutionaries against the British, the Vietcong against the Americans, and the Palestinians/Hezbollah against Israel. It has also been a proven fact that where the opponent has found ways to negate the advantages of superiority through recourse to Grey Zone war, conventional forces have found it expedient to organise and train the military to fight like their non-state enemy foes through special forces or pseudo gangs such was done in Kenya, Malaya, and erstwhile Rhodesia.[12] In India, such instances have been the use of the Ikhwan in J&K[13] and Salwa Judum in the fight against Left-Wing Extremism[14]. Though much maligned when some rouge elements among them ran amok creating strategic embarrassment, yet their tactical utility is indisputable. The adage 'fight fire with fire' has never been truer.

A common sight in traditional war is the stream of displaced persons moving backwards or out of a war zone where two armies are grappling. The civilians of the enemy country are expected not be targeted but pushed out of harm's way as much as possible. This has changed in the Grey Zone. Car bombs, ethnic cleansings, knife or truck attacks as in France, attacks such as on 26/11 in Mumbai or the frequent targeting of minorities in their mosques in Pakistan and Afghanistan is Grey Zone war deliberately and specifically targeting civilians.

Another changing concept of the Grey Zone is of private armies being used by governments where legally they cannot send their regular forces. Blackwater of USA and the Wagner Group of Russia are classic mercenaries with a corporate

legitimacy. As one podcast on this issue states, “Is this the future of war or is this a slippery slope that takes all the accountability out of the battlefield”?[15]

In the same manner that Grey Zone conflict is militarising the police, it raises fears of *constabularising*[16] the military. This fear is most profound within the army itself. Steeped in the Clausewitzean tradition of war, the army does not like to be involved in internal Grey Zone operations. It feels that it dulls its honed efficiency to fight the ‘real’ war on the borders. Civilian security analysts support this view for a different reason. They feel that the army with its culture of using unrestrained force may cause a situation to deteriorate. Both views are partially correct but out dated. The sort of Grey Zone threats that manifest in the present times, i.e. internal armed conflict and externally fuelled subversive conflict, pose a dangerous threat to the state. They need to be combated with all the means at the disposal of the state.

Conclusion

It is a cultural shock for an army to come to grips with a situation where the security apparatus of the state other than the army assumes equal primacy in the nation’s defence. While fighting in the Grey Zone, intra state, the army is made subservient to the political and administrative leadership and frequently made to operate under the chain of command of the police. This is at variance with the traditional concept of war where though under political control — the military of a country retains primacy.

As the world sees more of Grey Zone conflicts, it is inevitable that the size of the conventional armies will decrease; conversely the size of the police forces and private security providers will increase. In this war, the nature of weapons will become more precise, more destructive and more different. Cyber war and psychological war are now very much a part of the Grey Zone war armoury. Intelligence and the technical means to acquire it have become overarching. Perception management will be very important since it aids Sun Tzu’s dictum of winning without fighting. To win, targeting the minds of the population will be more important than physically harming them. More so, because this war is waged without violating borders and without a defined ‘front

line'. The enemy using unconventional means will strike to cause political, economic and militarily harm, rather than military harm alone.

This article does not make concrete suggestions for the way forward. It attempts to focus attention on this issue to generate considered thoughts for bringing out structural, legal and doctrinal changes which will ensure robust security for a country in the era of the Grey Zone warfare.

Endnotes

[1] Primo Levi, The Drowned and the Saved, (translated from the Italian by Raymond Rosenthal) London: Abacus, 1989.

[2] Operational Law Handbook. *National Security Law Department*, The Judge Advocate General's Legal Center & School, U.S. Army, Charlottesville, Virginia, 2020. P.8.

[3] Lieutenant General GS Katoch, PVSM, AVSM, VSM (Retd), Terrorism – the 'Grey Zone' of Chaos , USI Journal, Journal of the United Service Institution of India, Vol. CXLVIII, No. 613, July-September 2018.

[4] Toni Pfanner, "Military uniforms and the law of war", *International Review of the Red Cross,* March 2004 Vol. 86 No 853, P. 109

[5] Ibid, p.115.

[6] *Little Green Men* is the stereotypical portrayal of extraterrestrials. In this context this is a colloquial expression used by the media while referring to masked unmarked soldiers in green army uniforms wielding Russian military weapons and equipment within Ukraine. Clearly, they were Russian military, but it could not be legally proved that they are that.

[7] Agreement for Bringing Peace to Afghanistan between the Islamic Emirate of Afghanistan which is not recognized by the United States as a state and is known as the Taliban and the United States of America February 29. 2020https://www.state.gov/wp-content/uploads/2020/02/Agreement-For-Bringing-Peace-to-Afghanistan-02.29.20.pdf

[8] Bill Roggio, "Taliban Touts more 'Red Unit' Fighter Training on Social Media", *FDD's Long War Journal*. Apr 08, 2021. https://www.longwarjournal.org/archives/2020/04/taliban-touts-more-elite-red-unit-fighter-training-on-social-media.php

[9] ISIS, ISIL, Daesh, Islamic State in Iraq and Al Sham, Caliphate etc. Presently it is generally referred as only'Islamic State'.

[10] David Barno, and Nora Bensahel, Fighting and Winning in the "Grey Zone". 91 May 2015. *Fighting on the Rocks*. http://warontherocks.com/ 2015/05/fighting-and-winning-in-the-grey-zone/.

[11] Ibid. p. 144.

[12] Bill Bailey, "Hearts and Minds, Psuedo Gangs and Counter Insurgency: Based upon Experiences from Previous Campaigns in Kenya (1952-60), a (1952-60), Malaya (1948-60) & Rhodesia (1964-1979)", Edith Cowan University, *Australian Counter Terrorism Conference,* Nov, 30, 2010. Hearts and Minds, Psuedo Gangs and Counter Insurgency: Based upon Experiences from Previous Campaigns in Kenya (1952-60), Malaya (1948-60) & Rhodesia (1964-1979) (ecu.edu.au)

[13] Shazia Yousuf, Excerpt: Garrisoned Minds, a book on militarization's impact on women. This essay looks at Kashmiri counter-insurgents, Hindustan Times, S 03, 2016. Excerpt: Garrisoned Minds, a book on militarization's impact on women. This essay looks at Kashmiri counter-insurgents | Hindustan Times

[14] Arijit Mazumdar , "Left-Wing Extremism and Counterinsurgency in India: The 'Andhra Model'", *Strategic Analysis,* 2013, 37:4, 446-462, DOI: 10.1080/09700161.2013.802518

[15] Candice Rondeaux, Private Militaries (Wagner vs Blackwater)," *The Red Line Podcast.* Mar 2020, 71 minutes. https://open.spotify.com/episode/0nlt5lmbTd8q9tlW26zJbT

[16] Ibid. p.87.

[@]**Lieutenant General Ghanshyam Singh Katoch, PVSM, AVSM, VSM (Retd)** has extensive experience in counterinsurgency both in J&K and the North-eastern states of India. He is a MS in Defence Analysis from The Naval Postgraduate School, Monterey, California. He was the founding Director of the National Security Guard's Centre of Anti-Terrorism Studies in 2016-2018. Since 2018 he has been with the USI of India where he is also a Council member.

Airpower in the Grey Zone

Air Marshal Anil Khosla (Retd)[@]

The Grey Zone is characterised by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war. It is hardly new, however. The cold war was a 45-year-long grey zone struggle in which the west succeeded in checking the spread of communism and ultimately witnessed the dissolution of the Soviet Union.

– Unconventional Warfare in the Grey Zone
Joint Force Quarterly (1st Quarter, Jan 2016)

Abstract

Recent trends world over, indicate that national political objectives are increasingly being achieved by grey zone operations, without official declaration of war. The grey zone operations include multifarious forms of state sponsored activities that are being carried out in the metaphorical zone between war and peace, maintaining the threshold below that of conventional war. They are not limited to military domain and characterised by high degree of denial and ambiguity. World at large, and India, is in a grey zone conflict scenario and is likely to remain in it for a long time. Airpower can play a major role and can effectively be utilised in many ways in these grey zone operations. This requires a change in mind-set, organisational adaptation and some amount of capability enhancement, reorientation, and training. Finally, innovation and out of the box approach is essential to deal with grey zone situations and threats.

Introduction

Earlier days states or nations used to resort to open armed conflicts by declaring war, with the aim of achieving an objective using force. Recent trends indicate that national political objectives are increasingly being achieved without official declaration of war. There are multifarious forms of state sponsored activities that are being carried out in the metaphorical zone between war and peace. These grey zone activities have become a norm in the recent years. The grey zone warfare is best defined as an aggressor engaging in actions that circumvent traditional norms and laws of war, in the pursuit of political strategic objectives. The grey zone conflict operations are unclear and ambiguous in character, and are orchestrated in such a way that the threshold is maintained below that of conventional war. These conflicts are carried out in any of the multiple domains using variety of means as a weapon.

Air power, besides offensive use, can also be effectively utilised in many ways in non-conventional hostile situations categorised above. Various aspects of grey zone operations need to be deliberated from the point of view of airpower involvement. Certain amount of reorientation would be required in application of airpower in these grey zone situations supported by capability enhancement in certain fields.

Grey Zone Operations or Conflicts

Definition. Grey zone conflicts, also referred by some as shadow wars, have been defined in many ways. They are not formal or traditional conflicts or full-scale wars between nations or states. If war and peace were to be given the shades of black and white, then *grey zone operations or conflicts would fall somewhere in between the peace-conflict continuum.* One of the definitions of the grey zone conflict is ‘the contested arena somewhere between routine statecraft and open warfare’. Two major characteristics of grey zone conflicts are that the threshold is maintained below the level of full-scale war, and second that, the means of operations

are not restricted only to military actions. Varieties of instruments of power, often asymmetric and ambiguous in character, are used to achieve the objectives.

Means. Grey zone conflicts focus on the weaknesses and the vulnerabilities of countries being addressed. Aggressors use a hybrid approach to exploit their adversary's weaknesses through the use of Diplomatic, Informational, Military and Economic (DIME) instruments of power. The vulnerabilities could include weak economic conditions, internal disparities, ethnic alignments, and religious polarisation etc. Based on these vulnerabilities, local population, disillusioned elements or even the diaspora could be exploited. *The grey zone activities could be in the domain of politics, economy, social movements, diplomacy, cyber, space, information, psychological and / or communications.*

Characteristics. Grey zone operations are generally sub-conventional in nature employing irregular means. They could be overt or covert, carried out by proxy players or non-state actors. Ambiguity is essential to keep conflict in the space between peace and war, and the aggressors always endeavours to maintain a high degree of ambiguity and deniability. Invariably, these operations are conducted in multiple domains, at times using both kinetic and non-kinetic modes simultaneously. They generally include the nuances of other classifications of hostile actions like no war no peace, hybrid operation, asymmetric and sub conventional warfare etc.

Comparison / Differentiation. Grey zone conflicts, no war no peace (NWNP) operations and hybrid warfare are terms often used by security analysts and academics to describe prevailing hostile conditions between two countries. NWNP operations also fall in the same zone as grey zone conflict, but NWNP operations are generally referred to military actions whereas, grey zone activities could be in any of the numerous domains mentioned above. *Grey zone conflicts and hybrid warfare are other two terms which could be confusing. Grey zone is an operational environment encompassing the space between peace and war, whereas hybrid warfare is a strategy with reference to the threats and means that are exploited in multiple domains.* These threats and means could either be employed in full-fledged open war or in grey zone conflict

situations. At the same time, *grey zone conflict and hybrid warfare are not independent of each other, they are intricately linked to each other.*

India's Grey Zone Threat Scenario

India is a large and most diverse nation with two inimical neighbours. India's myriad problems provide innumerable opportunities for the belligerent adversaries to exploit in the grey zone. The increased radicalisation in the neighbourhood has further opened up new grey spaces. Grey zone tactics is being followed both by China and Pakistan using different means.

Pakistan. Pakistan is using the low-cost option of grey zone tactics against India by promoting violent extremist groups. These non-state actor groups get funding and training in Pakistan, to carry out irregular warfare against India. The spectrum of anti-India grey zone warfare emanating from Pakistan is wide ranging from disinformation and incitement to terrorism. The grey zone activities of Pakistan include propaganda, false narratives, cyber warfare, and encouraging internal dissent and terrorism, to undermine the Indian national security.

China. China is the master of grey zone operations. This type of warfare is embedded in her philosophy, strategic thoughts, and doctrines. China has further mastered the art of converting and using anything and everything into a weapon for grey zone warfare**.** China practices its famous three-warfare strategy, which encompasses non-kinetic means like psychology, media, and law warfare, to achieve political ends. China has been extensively using psychological warfare and coercion against India with the aim to subdue India without fighting.

Dealing Strategy. India a large democratic and bureaucratic state is perceived to be a weak spot, ideal for grey zone operations. It will lose out if it does not adapt to the changing nature of warfare. India must prepare to deter China and Pakistan from extreme forms of grey zone aggression. An important part of any grey zone response strategy is to undertake institutional reform. These organisational and structural reforms, need to be embedded in the

current structures, in a phased manner without causing too much of turbulence. A word of caution, a change for the sake of change due to peer pressure needs to be avoided. The change should be based on factors like our threat perception, technological threshold, economic conditions and geo-political environment. India must develop framework of strategic deterrence to deal with grey zone warfare.

Grey Zone Warfare Aspects: Relevance to Air power

Grey zone operations comprise of many components and are waged in multiple domains and dimensions.These domains may be widely dispersed like land, air, maritime, cyber, space and Information. Based on the uniqueness of each situation, aggressors would determine in which domain, they can achieve the greatest leverage in the grey zone. The goal of using these domains would be to fuse multiple tactics and techniques together to strain the opponent's resources and taking advantage of his weaknesses. *Cyber and Information domains are the most fertile domains for Grey zone operations.* A look at likely activities in these domains is required from the point of view of airpower application and involvement, i.e., how do these activities directly affect instruments of airpower and how can airpower be employed against in these situations.

Land Domain. The social space is generally the incubator for ideology and political aspirations, and it provides the necessary ingredients for any uprising or rebellion. Fuelling and supporting insurgencies is the most common grey zone activity. This may include covert or overt support resorting to arming, funding, espionage, infiltration and / or subversion. Resorting to terrorism overtly by the non-state actors has become a norm these days. These activities give rise to manmade disaster situations, requiring a rapid response. Airpower provides capability to respond with speed. Besides offensive application, airpower provides assistance to military and paramilitary forces, Special Forces (SF) and other state-controlled armed units. Transportation is the first role for rapid induction followed by sustenance. It can provide further assistance in terms of building up situational awareness [intelligence, surveillance, and reconnaissance (ISR)], setting up an aerial command post and

causality evacuation if required. All the roles and activities carried out by the air force during peace time under the purview of Humanitarian Aid and Disaster Relief (HADR) and aid to civil authorities, and other agencies, can be utilised in the grey zone warfare. Other aspect related to the land domain grey zone activities is the protection of airpower assets from terrorist attacks (like attack on Pathankot airfield).

Maritime Domain. Maritime domain can also be used in the grey zone conflict. Piracy, hijacking, sea borne attack by non-state actors on coastal targets or attacks on oil rigs etc. could be classified under maritime domain grey zone activities. Land domain disaster situations and response would also be applicable in the maritime domain. In addition disaster situations like oil slick management, sea platform fire fighting, maritime rescue and evacuation etc. could also be encountered. Air power instruments can be effectively utilised in assuaging these situations.

Aerial Domain. Latest challenge faced by the world, due *to grey zone operations in the aerial domain is the sub-conventional threat posed by aerial platforms like, unmanned platforms, drones, swarms, hang gliders and powered gliders etc.* These platforms besides being used for direct targeting are also being utilised in roles like ISR, smuggling and arms trafficking etc. In the last few years world over, concerted efforts are being made to deal with these threats. These threats need to be dealt in terms of development and employment of detection systems, anti-drone weapons / systems, engagement procedures and licensing and controlling regulations. Airpower operators, assets and systems are essential component in the entire response for mitigation of these threats.

Space and Grey Zone. Space based applications are being utilised in a number of fields like, communications, education, healthcare, navigation and ISR etc. to name a few. Increased reliance on these space-based systems also gives rise to certain vulnerabilities that have a potential for grey zone exploitation. Space operations are suited for grey zone use due to characteristics of ambiguity and difficulty in damage assessment. Anti-satellite warfare includes kinetic weapons like missiles and non-kinetic systems including jammers, laser

dazzlers or spoofing equipment. Denial of these systems would have a direct bearing on air warfare especially in terms of navigation, targeting and networked operations.

Cyber Domain. This is the most active domain even in peace time. It has the maximum potential for grey zone operations. Cyber domain has become a battlefield with cyber warfare becoming a significant component of present and future conventional and grey zone conflicts. Unlike physical attack, a cyber-attack can be launched instantaneously from anywhere, anytime with little evidence, it is hard to trace and has a high level of deniability. These characteristics make it an ideal and most favoured tool for grey zone operations. Cyber-attacks could be launched against vital infrastructure like banking, power sector and water resource management etc. or military systems and networks. Air power operations are essentially networked operations with platforms, weapons and systems networked in three dimensions (land network, aerial network and network linking ground and airborne systems). Moreover, these networks are further integrated with sister services and other agencies involved with national security apparatus and response. Denial of these networks could prove to be catastrophic and these need to be protected adequately.

Information Domain. The prevailing digital age consists of internet, social media apps, and portable electronic devices. The flow of information (or misinformation) is very rapid and availability is widespread. The narratives can be created, fabricated, changed, or manipulated, and circulated very quickly. This is Ideal and advantageous for the grey zone conflict operatives. Post-strike media scrutiny and dissection of Balakot strikes is a classic example, emphasising the importance of not only execution but also need to control the narrative. Airpower practitioners need to have a multi-discipline, multi-domain, institutionalised structure to address these concerns.

Airpower Utilisation in Grey Zone Conflict

Grey zone conflicts need a whole of government, multi-dimensional approach with the application of all relevant instruments of power at their disposal. Air power resources are an

effective military tool for statecraft, characterized by flexibility, lethality, reach, rapid response and creation of shock and awe by effect-based operations. Airpower offers the war fighting components resources that can cover great distances and gain desired lethal and nonlethal effects with great precision. Air power is dynamic in its application and its effects can be switched on or off at ease and it can play an important role in grey zone operational environment. In offensive role it can provide many options however, its utilisation is not restricted only to offensive role. Airpower can reinforce the nation's course of action against grey zone warfare, with involvement in several direct and supporting roles.

Offensive Application. Kinetic application of airpower in the form of aerial attacks is one of the options available to the decision makers. Generally offensive use of airpower on own soil is avoided as it causes further alienation of own people. Multiple options are available even for the aerial attack if so decided. These could be from fighter aircraft, helicopters, or unmanned platforms with a variety of weapons. In grey zone situation generally, precision weapons are preferred to avoid collateral damage.

Aerial Mobility. Grey zone situations usually necessitate rapid response making air mobility the preferred option. Airpower can place the ground force into the region where needed and when needed, while also sustaining a critical lifeline into and out of the deployment zone. Special Forces, disaster management teams, their equipment and relief material can be inducted speedily through the medium of air. Both fixed wing transport aircraft and helicopters of varying capability are required for these tasks. Situation may demand large scale expeditionary response or insertion of smaller rapid action teams.

Situational Awareness. High degree of situational environment is required in grey zone situations and SA is generally the first victim. It is further corrupted by psychological and propaganda warfare on all pervasive social media. Versatile and adaptable airborne ISR resources are essential to any hybrid campaign. Aerial recce platforms are useful in building the situational awareness through visual, photo and electronic reconnaissance, both by day and night. They have been utilised many a time to

ascertain location of trouble spots, disruption or blockades of railway lines and roads and breaches in canal etc. If required aerial command posts can also be established for coordination of the operations.

Casualty Evacuation. Occasions do arise when injured personnel needing immediate medical attention may be required to be shifted to places where such facilities are available. These may be during the day or night. Depending on the place of evacuation and numbers of people to be evacuated either fixed wing aircraft in ambulance role or helicopters or combination of both may be required.

Air Defence. Air defence is a role or task of the air force, which is carried out 24 X 7 not only during war but even during peace time. With the proliferation of unmanned and other smaller platforms the sub-conventional threats, have been added to the list of AD threats. The vital areas and vital installations need to be protected against these threats. The spectrum of AD threats and operations has increased in the grey zone operations scenario. Appropriate detection systems and weapons [like Close in Weapon Systems (CIWS)] would be required to deal with them.

Deterrence, Posturing and Strategic Coercion. These roles and tasks are performed by the airpower instruments in both war and peace situations. They have a large scope even in the grey zone conflict scenarios. The appropriate deployment of assets and flying of specific types of missions can be used for posturing and signalling of intent.

Defence Diplomacy. Defence diplomacy is conducted by means of defence cooperation, exchange of visits and joint exercises. Like war and hostile situations, they have a role in the grey zone conflict situations as well.

Capability Enhancement / Reorientation

Airpower is commonly associated with air-delivered firepower and expeditionary capability. Airpower has a major and decisive role, even in these grey zone situations and now the air forces, world over are equipping and optimizing for low- intensity grey zone conflict scenarios. Existing airpower resources offer a large number of options; however, there is a need for some amount of recalibration and reorientation. Certain areas also need capability enhancement. These areas could include capabilities to impose measured costs on adversaries, kinetic and non-kinetic capabilities, lethal and nonlethal weapons, assets protection, organisational adaptations, technology infusion and doctrinal changes.

- **Air Mobility and Logistics Management.** Rapid mobility and induction is vital in grey zone operational scenario. An all-round capability (i.e. heavy and medium lift, fixed wing and rotary wing, manned and unmanned delivery platforms, landed and air dropped) is required. A hub and spoke system of induction and subsequent sustenance works well. Helicopters play and important role in speedy delivery in area of poor connectivity. Large numbers of operating surfaces (helipads and heliports) are beneficial especially in high terrain friction areas. Civil aviation assets with appropriate modifications need to be integrated in this effort. Integrated logistics management systems are equally essential. Automated logistics handling and disbursement ports would enhance the capability further.

- **Surgical Offensive Capability.** Offensive application of airpower invariably will be surgical in nature i.e. with precision avoiding collateral damage. Smart weapons with high degree of accuracy and adequate standoff are highly desirable. Standoff and precision capability enhancement is a continuous process and more the standoff better it is. Variety in type and extent of warheads provide more options in terms of effect generated. Air delivered, non-lethal, weapons are also needed in the inventory, as certain situations would require their use. Delivery platforms are also important. Unmanned Combat Aerial Vehicle (UCAV) capability is useful

in quite a few situations. Real time intelligence would be essential for kinetic force application.

- **Situational Awareness Enhancement.** Aerial reconnaissance and surveillance is the best way of obtaining the correct and current picture of the developing situation. Better SA can be obtained by keeping greater area under multiple sensor surveillance with better resolution. Intelligence and surveillance capability needs to be enhanced across the spectrum starting from humint to space based surveillance. Aerial vehicles, surface movements, maritime domain, communications and electronic signals need monitoring and all inputs amalgamated to produce a comprehensive battle space picture. Artificial intelligence needs to be embedded in the analysis systems to provide the desired end product on need to know basis, with decision support systems and what if options. Real time monitoring may be required to take on dynamic targets of opportunity. A Joint Surveillance and Target Attack Radar System (Joint STARS) is highly critical to the success of operations in hybrid warfare.

- **Protection and Security.** The Airpower assets could themselves be targeted in the grey zone warfare. These vital and costly assets would need security and protection from conventional aerial vectors, sub-conventional aerial threats and ground attacks. Multi layered security systems would be required for both aerial and ground threats. The aerial threat mitigation would need systems like CIWS on one end of spectrum to Ballistic Missile Defence (BMD) on the other end. Multiple threat handling systems like S-400 would be ideal for protection of cluster of VA / VPs. Automated, networked, technology based security systems would be required for the ground security.

- **All Weather Day and Night Capability.** There is no differentiation between day and night for grey zone activities. Ability to launch and use airpower assets in all types of weather and during day or night is very essential. Night vision devices can prove to be a force multiplier in this respect.

Portable lighting systems can be of immense use especially in helicopter operations.

- **Special Operation Platforms.** Aerial platforms like C-130 have a lot of utility in grey Zone conflicts. They can be employed in a variety of roles, ranging from logistical transportation to operational tasks like Special Forces team insertions and extraction, airborne command post, aerial cover, fire fighting and medical evacuation etc. Their ability to operate from short and unprepared surfaces, adds to their versatility. Roll on roll off kits are available for some of the roles mentioned above and can prove to be economical and practical.

- **Networking and Cyber Domain.** Air operations are highly network centric. In grey zone operations flow of information to numerous stake holders is especially important. Integrated networks with good architecture, supported by suitable applications will assist in building situational awareness, planning, communicating, and monitoring of situation in real time. The information flow would have to be needed to know basis to avoid paralysis due to information overload. The networks would have to have redundancies and protection measures in terms of firewalls and anti-virus systems. Monitoring control rooms with Quick Reaction Teams would help in ensuring their continued availability during hostile activity.

- **Space Based Capabilities**. The term airpower has changed to aerospace power with the aerial warfare envelope expanding to the domain of space. Space based systems and applications are embedded in every aspect of aerial warfare. In Grey zone warfare the involvement of space-based equipment and systems is on an even larger scale. From airpower operations point of view the most important capability enhancement required is in the space-based surveillance capability. Enhancement is required in terms of revisit and resolution, converting reconnaissance capability into surveillance capability.

- **Psychological War and Media.** Psychological warfare or perception war is a vital component of Grey Zone operations and is deeply embedded in them. Media engagement plan and organisational structure needs to be in place for perception management and narrative control. All stake holders need to work collectively in sync with each other. Appropriately equipped and manned operations room working round the clock is necessary for monitoring and conducting these operations.

- **Organisational Adaptation.** Organisational adaptation is required for managing the grey zone conflicts and operations. Appropriate organisational structures need to be created to investigate aspects related to information warfare, electronic warfare, cyber and space operations, strategic and Special Forces operations and technology fusion. Intention would be to develop a multi-domain rapid reaction mechanism. A proactive approach will be even better. A multi-discipline body like an aggressor group could be formed with a charter to monitor the environment, play devil's advocate by identifying possible threats and generating possible grey zone scenarios.

Conclusion

The world at large and India in particular will be in grey zone conflict scenario for a long time. Airpower has a major role in these grey zone operations. There is a need to be prepared to tackle unpredictability and not get surprised. This requires a change in mind-set and some amount of reorientation and training. In grey zone operations anything can be turned into and used as a weapon therefore, all the contingencies cannot be predicted. The need of the hour is to develop a high degree of resilience, so as to adapt to changing situations rapidly. Finally, innovation and out of the box thinking is essential.

References

1. Synergy, Journal of the centre for joint warfare studies, Feb 2020.
2. Aerospace and grey zone warfare, Air Mshl Anil Chopra, PVSM, AVSM, VM, VSM (Retd)

3. https://warontherocks.com/2019/04/blurring-the-line-part-iii-airpower-applications-in-the-gray-zone/
4. https://www.airforcemag.com/article/1009hybrid/
5. https://cenjows.in/upload_images/pdf/Synergy_Aug_2019_BW.pdf
6. https://www.japcc.org/countering-hybrid-threats-with-air-power/
7. https://secure.afa.org/Mitchell/presentations/050109hybrid_slides.pdf
8. https://www.sldinfo.com/wp-content/uploads/2016/01/Airpower-and-the-Hybrid-Threat.pdf
9. https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/
10. https://media.defense.gov/2017/Jun/19/2001764908/-1/-1/0/AP_0002_GRAY_AIRPOWER_ADVANTAGE_FUTURE_WARFARE.PDF
11. https://www.bournemouth.ac.uk/news/2019-06-17/explainer-what-hybrid-warfare-what-meant-grey-zone
12. https://www.airforcemag.com/gray-zone-conflict-drives-space-weapons-development/
13. https://defense.info/re-shaping-defense-security/2020/11/raaf-prepares-for-gray-zone-operations/
14. https://cenjows.in/upload_images/pdf/Synergy_Aug_2019_BW.pdf

@**Air Marshal Anil Khosla, PVSM, AVSM, VM** retired as the Vice Chief of the Air Staff in Apr 2019. A fighter pilot, he wields the pen with equal adeptness as he can wield the joystick. He holds two MPhil degrees on defence and strategic studies and is currently pursuing a PhD on China. An ardent blogger (Air Marshal's Perspective) and Sudoku player, he has pursued the latter 10 times up to the national level.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

Dragon in the Misty Land, Chinese Influence in the North-Eastern Region: A Critical Analysis

Major General Vijay Ranade[@]

"China's role in the North-eastern India is not to create instability but 'to maintain instability' because it wants to keep India out of Myanmar."

—— *Bertil Lintner*[1]

Abstract

This article is an abridged version of the paper titled "Dragon in the Misty Land, Chinese Influence in the North-Eastern Region: A Critical Analysis" by the author. The article outlines that the initial Chinese support to the insurgent movements in the Northeast (NE) of India followed the classic communist doctrine of supporting revolutionaries. It draws upon the Chinese psyche built up over generations through their cultural background including the game of 'Wei Qi' which imparts in their strategic thinking a 'Grey Zone' quality. The author brings out that the NE Region requires a cogent approach in all spheres, especially in infrastructure development and opening up the region for industry. The fault lines based on ethnic divergence and porosity of the borders and developmental deficit make it a challenging task for the administrators and security establishment to usher in peace as these vulnerabilities can be exploited by grey zone actions.

Introduction

At its inception, Chinese support to the insurgent movements in the Northeast (NE) of India followed the classic communist

doctrine of supporting revolutionaries. Unlike in other parts of the world, these revolutionaries were not communists at heart. The main group in Nagaland, National Socialist Council of Nagaland (NSCN) while being revolutionary in character was hardly communist as their main slogan was the non-atheist 'Nagaland for Christ'. Most groups were organised into quasi-military units with uniforms, ranks and organisations. These were both over ground and underground. Over a period of time as strategic dynamics changed, the Indian state managed to resolve some insurgencies and reduce others. With growing integration of the NE, the insurgencies have lost the revolutionary fervour. Today, the insurgent groups in the NE have lost the basic agenda for their movements and have become extortionist profit making bodies with focus on an industry called narco and arms trafficking.

Enter the Dragon

A popular Chinese game called Wei Qi[2] or Go is an abstract strategy board game, for two players, in which the aim is to surround more territory than the opponent. As per popular belief, it teaches the art of hiding intentions which should never be disclosed. The Chinese play the game of Wei Qi in their dealings with neighbours and its foreign policy in general.

Wei Qi. The game involves the art of deceiving the adversary, hiding intention and looking for solutions in the areas not addressed. This seems to be the Dragon's approach conforming to the Chinese master strategist, Sun Tzu who said, ''the supreme art of war is to subdue the enemy without fighting.'' China has used this strategy with great success. It has used its military power not for war but for successful military and diplomatic coercion. It seems the Chinese leadership plays this game rather well by hiding the intentions. Its forays in Doklam and now in Eastern Ladakh seem to be a long-term strategy aiming to strike at place of their choosing. Having redrawn the Line of Actual Control (LAC) in several Ladakh sectors, China is now seeking to replace the term LAC with the looser expression 'border areas'. It had its way in the Moscow 'agreement' of Feb 2021 on the side lines of a Shanghai Cooperation Organisation (SCO) meeting, which repeatedly mentions "border areas," not LAC.[3] All the boundary-related bilateral accords and protocols are LAC-centred.

But it appears that China is treating the LAC as a line to actually control by changing facts on the ground. The Moscow agreement's use of the vague term "border areas" helps obscure China's encroachments and creates space for more Chinese salami-slicing[4].

The One Belt One Road (OBOR) and Belt and Road Initiative (BRI). OBOR and BRI are gambits in a fresh game of Wei Qi. It is a strategy for hegemony on land and sea, in particular in the Indian Ocean. According to the sources, the BRI involves over 70 countries and is bigger than US Marshall Plan to rebuild Europe after WW II. The Indian Ocean has major traffic going through its waters namely the container traffic and the oil shipments. With the BRI coming in, China can become the dominant power in the Indian Ocean with the wherewithal to influence this traffic. China has established links in Myanmar. The recent coup there will expedite the growth in Chinese influence there as Western business stays away. Resultantly, China is now better placed in expanding its influence over the region through Myanmar. The maritime BRI link passes through South China Sea and the Indian Ocean. To facilitate this, China has developed porting facilities up to Djibouti through Kyaukpyu in Myanmar, Hambantota in Sri Lanka, and Gwadar in Pakistan. These ports, if required, can be used to station naval war ships. These overtures will have major bearing on the delicate and sensitive NE Region.

As stated earlier, Sun Tzu's dictum of subduing without fighting is being pursued single mindedly by China. It has used its military and economic power not for war but for successful military and diplomatic coercion. Its overflowing coffers enable it to apply the dictum with greater effectiveness without overtly making its aggressive intentions clear. This is the grey zone which China is using. China's unchecked military intrusions and transgressions across the disputed border are examples of its military coercion. China, to establish its hegemony in the region, has made aggressive diplomatic manoeuvres with Myanmar and Nepal with an aim to undermine India's standing with these countries. These countries straddling the NE Region are very important in the internal dynamics and balancing of equations. China has been making inroads near the Indo Nepal bordering Lapcha – Limi area,

as reportedly People's Liberation Army (PLA) has constructed buildings in Humla district in Karnali province which is important for the pilgrimage to mount Kailash, a bargaining chip with both India and Nepal. Along with making roads, China has been diverting the course of some of the mountain rivers flowing into Nepal.[5] While earlier China was engaging India only through the NE, now it is also engaging India through Nepal.

Water as Weapon. The use of water as a weapon is a clear grey zone move. In the absence of legal water sharing agreements, the adverse effect of reducing lower riparian water cannot be effectively countered. The large-scale construction of dams and river connectivity projects by China pose a serious challenge to water security, not only to NE but South Asia as well. Challenges due to the use of water as a strategic weapon by China in the absence of any worthwhile treaty loom over South Asia. The measures adopted by China to use the water resource of Tibet as its sovereign property are a cause of serious strategic and security concern. Post-Doklam standoff, China had refused to share hydrological data on the Brahmaputra, (Yarlung Zangbo in Tibet), while it shared the information with Bangladesh. China's media reported on 30 Nov 2020 that authorities have given the go-ahead for a Chinese hydropower company to construct the first downstream dam on the lower reaches of the Yarlung Zangbo in Tibet, marking a new phase in China's hydropower exploitation of the river with potential ramifications for India.[6] The rivers in China give them an advantage in South Asia to use water as bargaining chip for any strategic or economic coercion. With such storage of water, China will have some capability to release extra water when India does not need it and stop the same when it faces water shortage. Water pollution is another concern. It is, therefore, necessary that a water treaty must become a crucial subject of discussion with China bilaterally.

Grey Zone Operations

It is not clear what China's intentions are behind its BRI. Is it a well-laid and finely orchestrated plan to extend Chinese hegemony over much of the developing world? This is what its critics claim. Or, as the Chinese assert, is it simply an attempt to replace America's worldwide domination with a multipolar order

where there is a more efficient allocation of resources and integration of markets which everyone would benefit from?[7] So, the equation is the fulcrum called the NE states between China and India. Holding or engaging India elsewhere will keep Indian attention and energy from stabilising the NE. It will prevent India from its efforts to use the region as the launch pad to reach out to Southeast Asian Region through Myanmar. Veteran journalist-writer Bertil Lintner had said, China's role in the North-eastern India is not to create instability but "to maintain instability" because it wants to keep India out of Myanmar. China uses military coercion, intrusions and transgression at various points on the disputed Mc Mahon Line[8] / Ardagh-Johnson line[9].

End Game

The NE is a region which holds promise for the Chinese to use grey zone operations against India. It can keep India distracted while it establishes a presence at Kyaukpyu in the manner it has done at Gwadar. Once done, India's East and West coasts will face a vulnerability that they have not faced since the Europeans came to our shores in the 16th and 17th centuries. Our NE, which is geographically located at crossroads and is a fulcrum to India's forays into Southeast Asian Region, will stand bypassed and diminished. Stability and development of this launch pad is essential for the policy of Look East / Act East to succeed. There is a need to address the region holistically and look for an inclusive approach to all the issues. The Look East and now Act East have a lot of promise to find an inclusive solution to the region but it requires stability which is elusive at least at the moment till the insurgent groups come into peace agreements with the government. Chinese grey zone strategy will aim to ensure that such stability is always interfered with. The security dimension needs to be addressed holistically and strategically. India needs to be sensitive to the possibility of the Chinese using this gambit and stymying it by allocation of attention, resources, and development to long delayed initiatives in the NE. The accessibility to, and within, the NE through the road and surface communications requires urgent attention. The weak industrial base and economic zone not supported by developing infrastructure makes it difficult to make it self-sustaining.

Proactive Engagement. The NE Region requires a cogent approach in all spheres, especially in infrastructure development and opening up the region for home grown industries under 'Vocal for Local'. The region is rich in raw materials and an attractive target for the anti-national elements. The fault lines based on ethnic divergence and porosity of the borders and developmental deficit make it a challenging task for the administrators and security establishment to usher in peace. All-inclusive approach addressing all the spheres like development, aspirations of the people, addressing the issues raised by the insurgent groups within the framework of the Indian Constitution is the need of the hour.

The region has abundance of the minerals, gas, oil, and hydro power which is waiting to be harnessed and once done, it will not only change the face of the region to prosperity but address all the aspirations of the people. This development will also give India the power to extend its gains to Myanmar and Bangladesh e.g., Tipaimukh Dam in Manipur once completed will not only power the region but it will be surplus for the neighbours. The region is surrounded by Bangladesh, Myanmar, and Nepal, which would have direct adverse economic bearing in case Chinese actions destabilise it. Therefore, it is of utmost importance that in our strategy to enhance the Look East / Act East venture, Myanmar and Bangladesh must be taken on board. The entry to Indian Ocean is through Bay of Bengal and India, Myanmar and Bangladesh are the littoral states in the bay. The shortest route from China to the bay is from Kunming / Chengdu Region. Chinese state-owned firms have reached agreements with Myanmar to construct a $ 7.3 billion deep-water port and $ 2.7 billion industrial area in a special economic zone at Kyaukpyu along the coast of the Bay of Bengal. The strategic town is the terminus of a $ 1.5 billion oil pipeline and parallel natural gas pipeline running to Kunming in China's Yunnan Province.[10]

Conclusion

Chinese unconventional operations can have traction in the NE Region because of the enabling factors there. Some of these factors are vestiges of history and some a result of lack of effective governmental control by states due to the tribal nature of society and traditional tribal laws. The Kyaukpyu project helps Chinese to avoid the vulnerable Malacca strait. China needs pliable countries to further the aim of BRI by connecting the surface BRI to maritime BRI and dominating the world's busiest and crucial sea lines of communication, the Indian Ocean and Malacca strait. Indian stability in the region would effectively check China in the NE Region. Any stability will benefit from our positive engagements with Myanmar and Bangladesh. Only then we will be effective in Acting East for the security and prosperity of all smaller countries in the region and pre-empt any grey zone actions.

Endnotes

[1] Bert Lintner, The Great Game East: India, China and the Struggle for Asia's Most Volatile Frontier, (Noida, India: Harper Collins 2016)

[2] Wei Qi (Mandarin for 'board game of surrounding') had its origins in China sometime before 500 BC. Wei Qi, probably better known as 'Go!' is a game which occupies a place in Chinese history and culture. The basic aim of the game is to capture as large a territory as possible on the board.

[3] Brahma Chellaney, "On China, India is making a mistake" *Opinion, Hindustan Times* Sep 18, 2020. https://www.hindustantimes.com/columns/on-china-india-is-making-a-mistake/story-QPxd0o3RJKhgzghOm7mX1I.html

[4] Ibid.

[5] Shishir Gupta, "China road projects changed course of rivers, expanded its territory: Nepal govt document", *Hindustan Times,* Jun 24, 2020. https://www.hindustantimes.com/india-news/china-road-projects-changed-course-of-rivers-expanded-its-territory-nepal-govt-document/story-NGEiAQc25H1 oIcCXEgu4GI.html

[6] Ananth Krishan, "China hydropower company plans first downstream dam on Brahmaputra", The Hindu, Nov 29, 2020. https://www.thehindu.com/news/international/china-hydropower-company-plans-first-downstream-dam-on-brahmaputra/article33206687.ece

[7] Bertil Lintner, *The Costliest Pearl: China's Struggle for India's Ocean*, (London:Hurst and Company, 2019).

[8] The McMahon Line is the demarcation line between Tibet and the North-east region of India proposed by British colonial administrator Sir Henry McMahon at the 1914 Simla Convention signed between British and Tibetan representatives.[1] It is currently the generally recognized boundary between China and India, although its legal status is disputed by the Chinese government.

[9] The Ardagh–Johnson Line is a proposed boundary of Kashmir abutting Chinese Turkestan and Tibet. It was formally proposed to the British Indian government by Major General John Ardagh, chief of military intelligence in London, in 1897, based on the surveys conducted by William Johnson in 1865. The Ardagh–Johnson Line is one of three boundary lines considered by the British Indian government, the other two being the Macartney–MacDonald Line and a line along the Karakoram range. The British preference among the three choices varied over time based on the perception of their strategic interests in India.

[10] Gregory. B. Poling, "Kyaukpyu: Connecting China to the Indian Ocean", *CSIS Briefs,* April, 2018.

@**Major General VS Ranade** is an artillery officer commissioned in 1984. After commanding an Artillery Regiment, he commanded an Assam Rifles Sector and a Mountain Division in the Northern Sector. He is a graduate of Defence Services Staff College where he also had an instructional tenure, Higher Command Course and Advanced Professional Programme in Public Administration course. Presently, he is the IG (Operations) in the National Security Guard.

The Determinants of India's National Military Strategy

Lieutenant General (Dr) Rakesh Sharma (Retd)@

Editor's Note

This is an abstract of the USI National Security Paper 2020.

Introduction

The enunciation of a nation's short and long-term security strategies is dependent on the geo-strategic environment. Conversely, failure of security strategies is also due to inappropriate assessment of the environment.[1] Therefore, in order to formulate a long-term military strategy, it is imperative to have holistic visualisation of the principal regional threats and challenges, including asymmetric ones, transnational threats, and even unanticipated ones! India is geographically located in a challenging strategic environment which argues for a strong and effective military force capable of defending territorial integrity and sovereignty. In a democratic dispensation like India, conduct of a military campaign will always be a political decision dictated by security considerations which are interpreted through a political lens.

Security Strategies

Military strategy cannot be viewed in isolation as in the prosecution of the national security policy, the military is one instrument along with other parameters of national power — diplomacy, economic leverages, political strength and will — cumulated with soft power. In a multi-domanial warfare environment, Joint Military Strategy (JMS) must become part and parcel of the mother document, the National Military Strategy (NMS), which by itself will draw from the National Security Strategy (NSS) which would bring all elements of national power together. In the Indian context, it is opined that the new structure

of the Department of Military Affairs (DMA) has been established seamlessly in the Ministry of Defence (MoD). Creation of two separate strategies — the National Defence Strategy and NMS — will only lead to hair-splitting of thought processes and duplication within a deemed near-singular establishment! NMS, hence, would envisage employment of all the nation's military and civil capabilities at the highest of levels and long-term planning, development and procurement to create the requisite capabilities to assure victory or success.

The South Asian Geography

The Transition of Strategic Geography. The strategic geography of the South Asian Region is undergoing intense strategic transition due to the Chinese Belt and Road Initiative (BRI) and the geo-strategy of Indo-Pacific. The BRI is the most significant engine of China's geopolitical ambitions, and South Asia is at the heart of it. While Covid-19 has moderated the BRI, it has not put it on the backburner. In the coming decade, several projects will fructify, though some may get jettisoned for various reasons. The geographic barrier of the Himalayas between Nepal and China, and Pakistan and China will be changed by railways, roads, and tunnels. China will push its technology and deep pockets to ensure that this infrastructure development will make the South Asian Nations dependent on it for a long period. Trans-Himalayan Economic Corridors will come into being, linking Nepal and Myanmar with China's Yunnan, Sichuan and Gansu Provinces and Tibet and Pakistan with Xinjiang and Tibet. This will allow intensive trade and interaction. As part of BRI, China has been building or upgrading ports all around India — in Kyaukpyu, Burma; Chittagong, Bangladesh; Hambantota, Sri Lanka; and Gwadar, Pakistan, and in many other countries in the Indian Ocean Rim.

The Geo-Strategy of Indo-Pacific. The Indian Ocean has the most critical sea lanes and choke points connecting Middle East, South and East Asia and Africa with Europe. It is no surprise that the major naval powers and regional navies have placed the Indian Ocean as a priority theatre in current and future operations, strategic planning and maritime security operations which include

counter-terrorist, counter-trafficking, and counter-piracy missions. The lexicon 'Indo-Pacific' has found its way into official documents. Indo-Pacific Region contributes more than half of the world's GDP and population and has huge natural resources and potential for new economic opportunities.[2] Indo-Pacific countries sharing a maritime border with the Indian Ocean Region (IOR) or the Pacific Ocean have objectives to deepen their strategic bonding by enhancing maritime connectivity through quality infrastructure. Though these strategies or initiatives might appear to be common goals of Indo-Pacific, however, there are some differences in approaches towards Indo-Pacific construct that calls for convergence in the areas of cooperation to achieve peace and security in the Indo-Pacific Region.[3] India's concept of Security and Growth for All in the Region (SAGAR) believes in an Indo-Pacific that is free, open and inclusive, and one that is founded upon a cooperative and collaborative rules-based order. It is also apparent that China will have to cover the IOR with its naval presence, hence increasing the possibility of naval engagement in the region.

Strategic Threats and Challenges

Undeniably, India will be a leading power in the foreseeable future. However, India is a nation that has unsettled borders, rapidly militarised maritime environment and is also incessantly deployed in countering infiltration and terrorism, and left wing extremism. The context of creation of a NMS, hence, has to be visionary and with far-reaching implications.

China. With pending intransigent boundary dispute with China, it is mandatory for India to explore how the relationship with China will unfold? The 2020 tensions in Eastern Ladakh predict a continuity of aggression and belligerent attitude of China in pursuance of its geopolitical ambitions. At the same time, goading its client and rentier state, Pakistan, to keep ratcheting up tensions in Kashmir aids these ambitions. In light of China's increasing strength and global presence, stronger possibility exists of a threat manifesting from China in the mid and long term. India, hence, can ill-afford to ignore China's increasing economic and military might, its assiduous strategic bases in IOR, deliberate lack of progress in the Sino-Indian border talks, and close economic and

military affiliations with Pakistan. The interregnum up to 2050, with many intermediate milestones, will be an era of major tensions with India which is a major geopolitical competitor in the periphery.

Pakistan. It is obvious that the anti-Indian-ness that is a DNA of the Pakistan Army – which virtually controls the polity of the nation – is unlikely to be done away with in the foreseeable future. Pakistan defines its security in tangible terms – as military capability to thwart a military threat from India, and provides legitimacy to the Pakistan Army as the custodian of nationalism. The geo-strategic location of the nation, grave asymmetries in development among the provinces and the extraordinary role that the Pakistan Army has played, compounds the anxieties of Pakistan presently, and in the future. Any great socio-political change in Pakistan that would lead to attitudinal change may not happen without attendant internal upheaval and instability. A more benign thinking in Pakistan in the foreseeable future is most unlikely. Pakistan would keep India embroiled in combating an intransigent Pakistan Army on the Line of Control (LoC) and the International Border (IB), and in proxy war in the hinterland. Pakistan, therefore, will remain an adversary in perpetuity and, hence, does mandate hard power considerations and a war-winning strategy.

The Collusive Threat. In matters of China-Pakistan collusion, Pakistan has already upgraded its security calculus with China through the China Pakistan Economic Corridor (CPEC). The collusive nuclear warhead-ballistic missile-military hardware nexus between China and Pakistan, described by both as an ‘all-weather friendship’, has grown to menacing proportions. With collusive support from China, Pakistan is also a testing ground for the latest Chinese technology, in the next conflict or even in peacetime. It would employ a combination of different types of warfare – conventional, insurgent, terrorist, Information Warfare (IW) and a concoction of military and non-military, kinetic and non-kinetic. The burgeoning nexus clearly indicates a unified front of the two adversaries, in the North and West.

The Maritime Frontier. China has created the world’s largest and modern navy in its attempt to expand its blue-water navy capabilities in the IOR. This points towards Chinese intent to

project power, seek to protect its maritime interests, and create a permanent naval profile in the IOR. These activities are portent of a future maritime arms race within the IOR and beyond. India, in all measures of contemplation, dominates the subcontinent and has the biggest role in the Arabian Sea, the Bay of Bengal and the IOR. India's central location in the IOR, in proximity to the sea lanes emanating from the Persian Gulf, the Malacca Straits and the Red Sea/Gulf of Aden, makes it the natural naval power. Indian diaspora in the IOR nations also has its significant diktats. India continues to be the dominant naval power, with vast responsibilities due to the extensive maritime trade, the island territories, vast coastline, and geo-political ambitions. India has, through diplomacy, strengthened strategic links with IOR littoral states, closer ties with US and its allies, and internally has built up its own military power to complement its strategic outlook. It necessitates that India continue with the build-up and modernisation programs of its maritime prowess including amphibious, maritime air and naval joint warfare capabilities.

Insurgencies and Terrorism. Aiding insurgencies and indulging in terrorism against India will remain a low cost option for Pakistan as it simultaneously affects India's rise as a major power, influencing her neighbours. The Kashmir issue, being kept in public consciousness in Pakistan, allows the army to remain relevant and a sole institution of merit. Pakistan also employs technological tools like cyber warfare, information distortion, psychological warfare and propaganda, applied on nearly daily basis, while retaining a modicum of deniability. Indian armed forces have been and will remain committed extensively in internal security, in combating terrorism and insurgencies.

India's Strategic Culture: An Overview

Strategic Culture is stated as a set of shared beliefs, assumptions, and modes of behaviour, derived from common experiences and accepted narratives (both oral and written), that shape collective identity and relationships to other groups, and which determine appropriate ends and means for achieving security objectives. Strategic culture and use of force are inseparable in most situations. Security today is no longer the responsibility of the armed forces alone. The world, in the post-Cold War period, has

been overtaken by the information technology revolution leading towards the formation of a knowledge society. Therefore, security as a notion has become all-pervasive and needs to be defined as the complex interaction between the culture and the capability of any nation-state.

India's strategic culture is a complex amalgam of historic myths and legends, and memories of ancient states and civilisations. "Discerning the underlying traits of India's strategic culture, its distinctiveness, and its resonance in India's contemporary actions may take some effort. But it can be done and [it is the], omniscient patrician type as opposed to others such as, theocratic, mercantilist, frontier expansionist, imperial bureaucratic, revolutionary technocratic, and marauding or predatory."[4] India is perceived as a pacifist, having historically never invaded other territories and having borne the brunt of many invasions. Indeed, strategic behaviour in dilemma could give an impression of pacifism and defensive mind-set. The larger Indian thoughts on strategy in India relate to strategic autonomy and sovereignty and nuanced approach to resolution of problems. The strategic culture impacts civil military interface, which is important in evolving NMS.

Civil Military Interface and National Military Strategy

Apparently civil-military interface and NMS are mismatched terms in India, as far apart as it allows one to be insulated of the other. In the existential routine peacetime functioning, the bureaucracy retains a deliberate and well thought out detachment from strategy, shielding themselves from accountability and responsibility, and the political hierarchy is mired in more pressing matters and not inclined to contribute to the military's conceptualisations and war games of an unknown future. In a democracy, like a thriving one that India is, civilian control – that is, by elected representatives of the people – is the absolute imperative. Civilian control allows a nation to base its values, institutions, and practices on the popular will rather than on the choices of military leaders, whose outlook by definition focuses on the need for internal order and external security. However, if military strategy is compounding of ideas to be implemented by military organisations to pursue desired strategic goals, then how

can the strategy be formulated in a vacuum? Civilian control over the military in India is presently addressed in multifarious ways. In matters of acquisitions and procurement, right from approval of acceptance of necessity to control on finances, on structuring, on promotional and human resource issues, and the like, civil control exists everywhere. However, the politico-bureaucratic involvement in the NMS must not be relegated to the time of involvement in combat. This needs to be constantly revised and updated in peace time.

Technology - the Driver of Future Warfare and Military Strategies

The prospective great transition in warfare can be ascribed to the newer technologies of the information age – largely the computer and internet. Land warfare in the future will be restrictive of large and heavy formations manoeuvring for deep thrusts in the plains and deserts. It will be an era when combat will, in addition to conventional forces, include militias, guerrillas, terror groups, precision weapons and information warfare. Technology is placing warfare on a decisive threshold to transit into new modernity, and to forecast new warfighting strategies. In future wars, machines will make life-and-death engagement decisions even without reliance on human interface. Taking the technological advancements in China as cue for futuristic study, the following aspects need taking cognisance off in formulating military strategy:-

- Robotic vehicles – many of which are autonomous – in maritime, aerial and land warfare.
- Information warfare.
- Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities.
- Precision guided munitions.
- Space warfare.
- New forms of delivering kinetic effect. Notably through lasers and electromagnetic rail guns.

- Cyber war.

Articulation of India's National Security Strategy

India does not, as yet, have a well-articulated NSS document for two reasons. These can be adduced as:-

- First, there is no political consensus in the country on national security issues.

- Second, the government has not been able to address the crucial issue of coordination required to formulate and address the issues of national security. The National Security Council lacks the power to enforce anything. There is no common understanding of what constitutes national security.[5]

India's NSS should establish the national long-term objectives, action programmes and resource allocation priorities, and envisage development and coordination of all national power instruments to achieve national goals in an ever-changing globalised environment. In the past, security strategy has often been focused on external threats, and more specifically external military threats (which therefore require a military response). As has been evident over some time, it is imperative to accept that what can be regarded as developmental or policy issue, can become a major security challenge, especially of the non-traditional kind.

Formulation of National Military Strategy

The conceptualisation argued above denotes creation of NMS with sufficient forethought and analysis, and not on a trigger. National military strategy is a plan that signifies utilisation of means and concepts of employment of national power and the military to achieve political ends. Politics creates war, so success or failure in war is ultimately the responsibility of the political leadership.[6] Military strategy in operational execution is a military responsibility, and stating the end-state is a political task. The duty of military leaders is to see that political leaders do not fail because they had poor advice. Hence, evolution of military strategy is two-way traffic between the government and the military professionals, in which, in a democratic dispensation like

ours, the final call will rest with the government. Hence, the government and the military together have to be accountable to the populace on the success, or otherwise, of the military strategy. As part of the NMS, there is a JMS that envisages utilisation of military force, denoted by the three services, jointly.

Joint Military Strategy

Almost all conflicts that India has fought have been essentially land wars in which the army has been the predominant player. The threats faced by the country have been focused across the border. Insurgency and low intensity conflict have also been in its domain. The air force, traditionally seen only as a supporting arm, has consistently sought an independent stature partly by refusing to get conjoined with the others, principally the army, and partly by stressing the strategic role of air power. The Indian Navy has a more fortunate position, operating, as it does, in a domain in which others can play only supporting roles.

What then is JMS? In ancient Greece, it was the 'art of the general'. In the USA, it is defined as the art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force, or the threat of force.[7] As stated earlier, JMS is a subset of the NMS. It can also been defined as consisting of joint objectives, ways and means, as an equation: Strategy = Ends + Ways + Means, broadly:-

- Ends - Objectives that the three Services strive for, gleaned from NSS.
- Ways - Joint courses of action to attain the objectives.
- Means- Optimal use of instruments by which ends can be achieved.

A country is said to have attained jointmanship of its armed forces if it institutionalises the following:-

- Joint planning, development of doctrine and policy-making.
- Joint operational commands and staff structures.

- Evolution of joint equipment policy and procurement organisation.

- Integrated preparation of budget and monitoring of expenditure – both capital and revenue.

- Joint training.[8]

JMS, hence, becomes part of the NMS that would signify integrated utilisation of military means and concepts of employment of military. Certain significant issues in formulation of JMS for India are as below:-

- In JMS, the ultimate objectives are those of the national strategy. While conventional wars may be passé or limited, the military hierarchy must involve the polity at the highest of levels – to obtain guidance and directions.

- Some may say that it is unwise, impossible, or even dangerous to enunciate openly a JMS. However, enunciation formally denotes arrival of India in international stage as a nation in league with others who do so. Military strategy may, however, be fully or partially declaratory and/or classified or even deceptional.

- JMS must be 'joint' in all its forms. It should be a cumulative utilisation of national power. It will be subsequently necessary to translate it into Service-specific concepts and plans, at the strategic and operational levels. In the operational level, it is all the more important that all corresponding tri-Services echelons must operate with full synchronisation.

- Long-range strategies must be based on estimates of future threats, objectives, and requirements, and are, therefore, not constrained or dominated in considerations by current force posture. Operational strategies must be based on joint capabilities and not on threats alone, as threats are examined by each Service autonomously.

Conclusion

21st century warfare is metamorphosing without a distinct pattern, where conventional war with increasing utilisation of Special Forces, irregular war and terrorism are not dissimilar, or with fundamentally different approaches. There is an increasing blurring of distinctions between war and peace, between the different domains of conflict (land, maritime, air, space, cyber) and between kinetic and non-kinetic effect. Cyber contributes to this blurring of the distinction between peace and war by creating uncertainty as to what constitutes conflict in cyberspace. They are multiple means of war employed in combination by the adversary and conducted by both state and non-state actors. The Indian armed forces are one of the most significant custodians of national security. After the military strategy has been enunciated, and while the operational directive is laid down by the political leadership, the actual planning of operations is left to the armed forces and in future, the theatre commanders under the Chief of Defence Staff.

Endnotes

[1] Tang Shiping, "A Systemic Theory of the Security Environmen". *The Journal of Strategic Studies*, Vol 27, No 1, March 2004, pp. 1.

[2] Prabir De and Durairaj Kumarasamy, "Emerging Perspectives of Indo-Pacific Initiatives", *RIS*, New Delhi, accessed jan Dec 20, 2020 from http://aic.ris.org.in/others/files/pdf/AICCommentary%20No%209% 20September_2020.pdf

[3] Ibid

[4] Rahul Bhonsle, "Jointness: An Indian Strategic Culture Perspective", *IDSA, Journal of Defence Studies, Volume 1 No. 1 New Delh*i, 2007, accessed Aug 12, 2020 from https://idsa.in/system/files/JDS1%281% 292007_0.pdf

[5] Arvind Gupta, "A National Security Document for India", *IDSA Comment*, accessed at www.idsa.in, 20 Oct 2011.

[6] Christopher Bassford, "Policy, Politics, War, and Military Strategy", *Marine Corps Doctrinal Publication 1-1, Strategy, 1997, available online at http://www.clausewitz.com/readings/Bassford/StrategyDraft/*

[7] JCS Pub. 1: Dictionary of Military and Associated Terms. Washington: U.S. Department of Defense, June 1, 1987, p. 232.

[8] Mrinal Suman, “Jointmanship And Attitudinal Issues”, *IDSA, Journal of Defence Studies, Volume 1* No. 1 New Delhi, 2007, accessed at https://idsa.in/system/files/JDS1%281%292007_0.pdf

@**Lieutenant General (Dr) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)** commanded a Corps in Ladakh – facing both Pakistan and China. He also served as was Adjutant General of the Indian Army. He lectures, participates in seminars, and writes in newspapers/military journals on geo-strategic environment, war fighting and military strategy.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

War: Yesterday, Today and Tomorrow

Brigadier Manoj Mohan[@]

Abstract

War has been an inalienable part of statecraft. However, its shapes and contours have been continuously evolving. From primitive bows and arrows to weapons of mass destruction, war has come a long way. A revolution in military affairs was unleashed a few decades ago with path breaking advancement in technologies and included interesting dimensions such as information warfare. This gave unparalleled advantage to advanced military powers as evident in the First Gulf war. Such advances are sought to be offset by circumventing strength by waging war through unconventional means. The emerging mean is 'Grey Zone' war. Application of grey zone war is likely to have a bearing on the very fundamentals of warfare. This article is an attempt to delve into the advancements in military relevant technology and juxtapose it with the way war is presently planned to be fought.

Introduction

War causes destruction and misery is a universally accepted fact, yet, ironically, it is also an inalienable part of statecraft. With that kind of indubitable and indisputable permanence, it is only the nature of war that keeps changing while its relevance remains intact. A change which is assuming increasing salience is 'Grey Zone' war. As per one definition, grey zone war encompasses, "Actions that do not quite fall under the clear definitions of 'War' by lesser levels of aggressions[… they are] not

to be confused with traditional methods of 'low intensity' conflicts between two opposing nation-states, grey zone conflicts are undeclared acts of international conflict that operate with an ambiguous approach[…] grey zone conflicts have numerous methods of approach, including cyber-attacks, occupation of land, use of biological and chemical agents, small scale terrorism and hostage situations".[1]

Historically the art of warfare and its methods of execution have kept evolving over centuries. Revolution in military affairs unleashed during the last couple of decades of 20th century once again brought in a profound change in the nature of warfare as it is to be fought in future. Today, information, hybrid, space, and asymmetrical warfare have become part of the latest generation of warfare where changes are taking place at astonishing speed, powered as they are by breath-taking technological evolution often in the civilian field. Any professional military will have to evolve and remain in sync with tomorrow's evolving nature of warfare so as to retain the ability to deliver when asked to do so. It is beyond dispute that technology shall be the biggest force multiplier in future wars. The Indian Army has ample exposure to conventional warfare—from world wars to 21st century. Certain internal disturbances and subsequent rise of insurgency and terrorism brought in a completely new dimension. The army has acquitted itself well and has a history of success in all forms of warfare. The crowning glory of course is the complete victory in 1971 which is now part of military folk lore. It is this victory, ironically that brings to fore the question captioned in the heading—can we fight tomorrow's war by celebrating past success? More so when in a nuclearised South Asian environment, all out conventional war is unlikely to be the norm.

Hybrid and Grey Zone War

The most recent conventional conflagration took place between Armenia and Azerbaijan in the Nagorno Karabakh Region. It was conventional in one sense, but unconventional in the other. This war was watched with great interest around the globe and is of particular interest to military thinkers and planners. It was primarily so since over a decade or so a perception was being shaped that

the world is moving away from conventional warfare inducing a sense of complacency. This short war has served as a wakeup call, more so in the Indian context. Also, worth taking note of are two seemingly unrelated incidents — assassination of Iranian General Qassem Suleimani in Jan and nuclear scientist Mohsen Fakhrizadeh in Dec 2020. Use of satellites, drones, artificial intelligence (AI) and remotely controlled operations in these two cases can no longer be seen as one-off instance but as integral part of future grey zone battlefield. This brings out that to view grey zone war through the terrorism lens only may be fallacious. Infringing laws of war and sovereignty using technology is part of the lexicon.

Technology. The military relevant technological trends likely to play a major role in next 20-30 years have been analysed in an exhaustive paper from Brookings Institution by Michael 'O Hanlon titled "Forecasting Change in Military Technology 2020-2040"[2]. He has listed almost all major technologies which may have a decisive influence on the future battlefield. Apart from drones there are numerous trends visible or emerging in key areas of military technology. These are in the field of sensors, of many different types, which gather data of relevance to military operations. Then there are the computer and communication systems that process and distribute that data. This is followed by major weapon platforms and key enabling technologies for those platforms. Further there are relatively new technologies which hitherto may not have been considered relevant by militaries e.g., offensive cyber capabilities, Internet of Things (IoT), network centric warfare, quantum computing, Anti-satellite missiles, directed energy weapons, and the list of path breaking innovations goes on. While this is pure technological empowering of the military, its application in a manner that enables deniability, or which is unexpected is what falls in the grey zone.

Another exciting domain with infinite possibilities is robotics and Artificial Intelligence. Small robots that can operate as swarms in all three dimensions-land, air or under water-may be capable of deciding when to offload their lethal munitions. For example, small robots that can operate as swarms on land, in the air, or in the water may be given certain leeway to decide when to

operate their lethal capabilities. By communicating with each other, and processing information about the enemy in real time, they could concentrate attacks where defences are weakest, in a form of combat that John Allen and Amir Husain call “hyper war” because of its speed and intensity.[3] Other types of swarms could attack parked aircraft; small explosives, precisely detonated, could disable wings or engines or produce secondary and much larger explosions. Many countries will have the capacity to do such things in the coming 20 years.[4] With Unmanned Aerial Vehicles (UAVs) that can fly 10 hours and a 1000 kilometre now costing only in the hundreds of thousands of dollars, and quad copters with ranges of a kilometre more or less costing in the hundreds of dollars, the trend lines are clear and the affordability of using many drones in an organized way is evident.[5] Although defences against such robotics will surely be built, at present they are underdeveloped against possible small UAV swarms.[6] And unless area defence allows for a certain part of the sky, sea, or land effectively to be swept clear of any robotics within a certain zone, it seems statistically likely that some offensive UAVs will survive a defender’s efforts to neutralise them - meaning that their capabilities to act as a swarm, even if perhaps a weakened one, will probably remain. Robotics with artificial intelligence may also be deployed on the battlefield in close partnership with real humans. These robotics could be paired one for one, or in larger numbers, under the control and for the purposes of a single soldier or unit.[7]

Drone technology particularly makes for an interesting study in view of demonstrated usage. Having identified its potential military usage, it has been a while since these have been inducted into various armed forces of the world — both in its armed and unarmed avatars. Arguably they were the single most important factor which tilted the balance decisively in favour of Azerbaijan. Videos of these armed drones swooping down on infantry soldiers, vehicle convoys, tank columns, artillery and air defence gun emplacements and so on creating destruction and mayhem on ground have gone viral on social media. Regulations for commercial or consumer drones for purchase are currently very rudimentary or lax. Anyone anywhere can purchase drones at a local hobby shop for personal use. Drone and micro drone

technology are easy to commandeer and inexpensive enough to add to their arsenal of effective weapon systems by shadowy organisations operating in the Grey Zone. Keeping in view the threats that could emanate from drones advertently or inadvertently, the Indian Civil Aviation authority has promulgated the National Counter Rouge Drone Guidelines[8] in 2019 and the Unmanned Aircraft Systems (UAS) Rules 2021.[9]

Indian Context

India has a volatile border, both to its East and West. The conventional threat from West as well as its manifestation is somewhat predictable while the unconventional threat is not. All along the border, scope for grey zone operations by the adversary exists. The use of drones to send weapons and drugs across, the terrorist-smuggler nexus are instances of the murky grey zone where the enemy can operate.[10] In case of our eastern adversary, the situation is somewhat more unnerving since the intentions and modus operandi remain inscrutable and opaque. This has been demonstrated repeatedly over a period of last two decades or so when we have been surprised by the adversary. There is a requirement for India to carry out restructuring and capacity building to meet the newly evolving threats.

Restructuring. The present structure of army has evolved over decades and withstood the test of time. However, in the same breadth it can also be said that the more the things have changed, the more they have remained the same. Our basic structure is a throwback to the world wars, a legacy we inherited from our colonial rulers. A large, unwieldy and monolithic organisation is an anathema and anachronism for the future milieu. Recent move towards relatively small, lean, flexible and integrated organisation is a step in the right direction. Special Forces are the need of the grey zone war times with their capability for stealth and deniability. Such capability also needs to be seen through the prism of terrain specific concepts and equipment given the wide variety of terrain obtaining in our context. A detailed study is required by experts in the field to examine the peculiarities of grey zone war afresh and suggest organisations adept to operate in the conventional and unconventional fields. The conventional army needs to disengage itself completely from the counter insurgency arena. Responsibility

for counterinsurgency operations must, therefore, shift to specialised forces like *Rashtriya Rifles (RR)* and the Central Reserve Police Force (CRPF).

Capacity Building. Capacity building should be multi-pronged albeit with the singular aim — decisive edge over recognised adversaries with meaningful deterrence capability. Two intertwined verticals need to be developed — intellectual and material — having a kinetic as well as non-kinetic version. The man behind machine has rightfully been recognised as the most important cog in the wheel, yet the machine itself can't be relegated to a secondary position as the recent conflict in Armenia has amply demonstrated. Acquisitions should now shift from heavy ordnance like main battle tank and long-range howitzers to precision and technology driven weapons/solutions. Use of third dimension must be factored in our acquisitions. Bottom line is that our inventory of weapon systems must reflect the shift from capture of real estate to debilitating the enemy. This is both physically and psychologically.

With grey zone war demonstrating its utility and an obvious requirement to be coordinated at the highest military and political levels, war can no longer be seen as 'military only' subject where others are only responsible for provisioning. Concept of dual use technology and harnessing of expertise in non-military domain must become part of our national security doctrine. Structures need to be built and greenfield projects launched for carrying out research in areas of emerging technologies and how these can be tweaked for furtherance in the prosecution of grey zone war.

Existing think tanks on strategic matters need to expand the themes of research to include perception management and cyber warfare as also use of space based and low-cost platforms.

Formal and structured technical collaboration with institutions like Indian Institutes of Technology (IITs) and Indian Institute of Science (IISc) needs to be worked out so as to facilitate identification and research in military related and/or multiple use technologies. Creation of cyber warrior teams consisting of students and young professionals who have the aptitude for the same would pay dividends for devising offensive or defensive

measures in the grey zone using commercially off-the-shelf technology. Opening new avenues for entry of domain experts even on a short-term contract for specific projects for which necessary expertise is not available within the services is a concept which will pay dividends.

In the grey zone war milieu, a military leader cannot function from an isolated silo any more, nor can the civil bureaucracy avoid taking their military counterparts on board in matters of national security. A short capsule at Lal Bahadur Shastri Academy may be considered for officers from the armed forces to aid better civil-military synergy as also to understand the strengths of the civil administration which can be leveraged for grey zone responses. It would also help in synergised response in times of unprecedented situations like the one in Galwan valley. This, with the use of technically 'non-lethal' weapons to circumvent agreed legal restrictions, was an obvious grey zone clash.

Brainstorming exercises are essential to identify future grey zone threats and validate counter concepts; however, the method of application of forces by the 'enemy' side must not conform to our comfort level but to the prevailing environmental realities. Identification of enemy's centre of gravity - militarily and in his society - is imperative so that a techno-military strategy could be adopted for it to be threatened. Radical ideas need to be encouraged and boundaries pushed rather than being conformist.

Conclusion

War is a serious business with direct impact on a nation's conscience and self-image, not to talk of the economic cost. We only have to analyse the wars on the opposite side of the spectrum to understand the above. On one end are the short, sharp and destructive conventional wars and on the other are the prolonged wars of counter insurgency and counter terrorism. While we as a nation justifiably feel euphoric and ecstatic about the former where we glorify their victories and tales of valour, scars of the latter are left behind not only on the military but also on many sectors of society in the alienation and bitterness or economic losses. The fast-paced technological evolution and the way it can be integrated into perception management require to be

factored in all war fighting philosophy and concepts. Therefore, introspection, keeping an eye on the changing environmental realities, and a constant assessment of own capabilities and limitations are required. Our entire perspective to war fighting needs course correction from time to time so as to remain in sync with the contemporary. The contemporary today and tomorrow encompasses grey zone war.

Endnotes

[1] David A Lemont, "Narrowing the Grey Zone Conflict Margin". *Master's thesis, 2019,* Harvard Extension School. https://dash.harvard.edu/bitstream/handle/1/42004082/LEMONT-DOCUMENT-2019.pdf?sequence=1

[2] Michael O'Hanlon. "Forecasting change in military technology 2020-2040". Brookings Institution Press, 2018. https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf

[3] JR Allen & A Hussain, "On Hyperwar." *Proceedings,* U.S. Naval Institute. Jul 2017, https://www.usni.org/magazines/proceedings/2017/july/hyperwar

[4] Michael O'Hanlon. Op cit.

[5] Ben Knight "A guide to military drones" Deutsche Welle. Retrieved may 21, 2021 from https://www.dw.com/en/a-guide-to-military-drones/a-39441185

[6]. K. Atherton). "As Counter-UAS Gains Ground, Swarm Threat Looms". *Aviation Week and Space Technology,* April 2018. 36-37.

[7] O'Hanlon, p.16

[8] National Counter Rouge Drone Guidelines. https://www.civilaviation.gov.in/sites/default/files/Counter_rogue_drone_guidelnes_NSCS.pdf

[9] The Gazette of India Extraordinary No. 133 New Delhi, Friday, March 12, 2021/Phalguna 21, 1942. https://www.dgca.gov.in/digigov-portal/Upload?flag=iframeAttachView&attachId=150337918

[10] Ramesh Balakrishnan, "India and the Crime-Terrorism Nexus", *Counter Terrorist Trends and Analyses,* Vol. 10, No. 9 (September 2018), pp. 11-17. https://www.jstor.org/stable/26487540?seq=1#metadata_info_tab_contents

@**Brigadier Manoj Mohan** was commissioned into the Infantry (The SIKH Regt) in 1986. He has served as instructor at the Officers Training Academy, Chennai and at Infantry School, Mhow. A graduate of the Defence Services Staff College, Wellington, the officer has held various prestigious staff and command assignments. He commanded his battalion in a high-altitude area in J&K and an Infantry Brigade in the deserts.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

Deciphering Grey-Zone Operations in Maritime-Asia[#]

Commander Abhijit Singh (Retd)[@]

Abstract

Recent grey-zone activity in maritime-Asia suggests an increase in hybrid warfare, even as the lines between military, economic, diplomatic, intelligence and criminal means of aggression become increasingly blurred. By replacing overt military aggression with soft provocations – kept well below the threshold of open warfare – aggressors attempt to leverage asymmetry, ambiguity, and incrementalism for strategic effects. These tactics are highly conspicuous in the context of South China Sea and the East Asian littorals, but even South Asia has had its own share of 'grey-zone' scenarios. To meet this challenge globally, there is a requirement to bring in a rules-based order.

Introduction

In recent years, the subject of maritime 'grey-zone operations' has drawn increased debate and discussion. The 'grey-zone' is a metaphorical state of being between war and peace, where an aggressor aims to reap either political or territorial gains associated with overt military aggression without crossing the threshold of open warfare with a powerful adversary.[1] The 'zone' essentially represents an operating environment in which aggressors use ambiguity, and leverage non-attribution to achieve strategic objectives while limiting counter-actions by other nation states.

For some time now, the organisation and approach of insurgent groups in the terrestrial domain has been one of

asymmetric attrition, whereby low-intensity and sporadic attacks have been launched against security forces. The strategic logic behind this tactic is that it is hard for the constituted government or occupying power to sustain the financial and political cost of high-security presence for any long period of time.[2] In a maritime context, however, these low-grade attacks have often been carried out by non-state actors and agencies in concert with military or coast guards in a way where the latter's involvement has been less than conspicuous.

Maritime Militias

The leading purveyors of grey-zone tactics in maritime-Asia are China's irregular maritime militias, dubbed 'little blue men' that seek to assert and expand Chinese control over an increasingly large area of disputed and reclaimed islands and reefs in the strategically important South China Sea.[3] These sea-borne militias, comprising hundreds of fisher folk in motor-boats, as well as China's paramilitary forces, are based mainly on China's Hainan Island and have been involved in "buzzing" US navy ships and those of neighbouring countries with rival territorial claims.

The idea behind Chinese militia operations is to exert authority over a maritime space using civilian craft and personnel but doing it in a way that precludes open military confrontation. By acting assertively and unprofessionally in the vicinity of other states, China's Coast Guard boats and fishing vessels seek to assert dominance in areas surrounding disputed features. Their activities are consciously kept below the threshold of conflict, yet demonstrate China's resolve to establish control over disputed features.

After Chinese maritime militias assisted in the seizure of the Scarborough Shoal in 2012, Beijing expanded its 'hybrid' operations in the South China Sea. China also began using its irregular forces to deter US freedom of navigation operations (FONOPS) in the South China Sea.[4] Notably, even as Chinese militias were professionalised, they maintained an ambiguous civilian affiliation, enabling Beijing to plausibly deny grey-zone activity. China has since resorted to illegal reclamation of features in the South China Sea, gradually militarising artificial islands in a

bid to establish de-facto control over their surrounding waters. In effect, say maritime observers, China's structured 'irregular tactics' have allowed Beijing to undermine international law and set precedents in its favour.

While the focal point of China's irregular warfare is the South China Sea, the East Sea too has witnessed a significant amount of militia activity. Following Japan's "nationalisation" of three uninhabited islets in the Senkaku group of islands in September 2012, there has been a marked rise in Chinese government vessel activity in the East Sea.[5] In August 2016, China demonstrated the effectiveness of grey-zone operations by sending over 200 Chinese fishing vessels into the Senkaku seas. In four days, a total of 28 China Coast Guard (CCG) vessels escorting the fishing boats are said to have entered Japan's territorial seas near the Senkakus[6]. Despite ending peacefully—with no landings on the disputed islands—the operation provided a glimpse of what Beijing's long-feared, potentially escalatory grey-zone tactics were capable of achieving in a distant Japanese dominated littoral.

Hybrid or Grey Zone?

Naval analysts also use the term 'hybrid warfare' in describing irregular maritime tactics. The origins of 'hybrid war' go back to 2005, when James N. Mattis, the present US defence secretary, and National Defence University researcher Frank Hoffman introduced the term into the security discourse, calling it "a combination of novel approaches—a merger of different modes and means of war."[7]Since then, the use of hybrid warfare techniques has expanded significantly, to include an entire spectrum of threats ranging for Russia and Iran's blend of military and paramilitary tools, to China's use of a 'grey zone' approach in its near-littorals, as well as the 'net-wars' launched by anonymous states and non-state actors.[8]

While 'hybrid' and 'grey-zone' connote two different conditions, in the context of asymmetric maritime operations, they have frequently been used interchangeably. Retired US Navy Admiral James Stavridis, for instance, argues that "Chinese activities in the South China Sea is hybrid because it represents a

'non-kinetic' attempt at influencing strategic competition in maritime-Asia and Europe".[9] Others have explained 'grey-zone' operations as an adversary's penchant for strategic ambiguity, whereas 'hybrid' describes a combination of conventional with irregular instruments of warfare, both in the strategic and political domains.[10] However one defines the two terms, both emphasise asymmetric tactics in the maritime domain.

One of the defining features of asymmetric threats in the maritime domain is that it is often backed by the ability to use other stronger means, as is the case with China. The communist party state, however, is not unique in this respect. In the case of the Iranian Revolutionary Guard Corps Navy (IRGC) too, the asymmetric threat is buttressed by the official power of the Islamic state. The reason Chinese and Iranian militia forces are effective in offsetting stronger opponents is that they are both backed by regular naval forces.[11] Yet, not every irregular force enjoys this advantage. The Sea Tigers of the LTTE movement (The Liberation Tigers of Tamil Eelam), for instance, could not sustain their attacks on the Sri Lankan navy because they lacked the flexibility and tactical agency that comes with the support of a powerful maritime force.

In part, the effectiveness of Chinese maritime militias owes to the active support of the Chinese Coast Guard. With the backing and guidance of CG cadres, China's irregular forces have assisted in reclamation activities around disputed islands, provided escort services to fishermen in contested waters, and even challenged oil rigs and non-Chinese military presence in the South China Sea. All aspects of militia operations in the South China Sea and East Sea are reportedly controlled by the higher echelons of China's military leadership.[12]

In Southeast Asia, it is unclear if Vietnam, Indonesia and the Philippines will be able to harness their fishermen to stage asymmetric attacks in the same way as the Chinese militias. Part of the reason is the absence of hard military power to back militia operations. Still, this does not mean asymmetric forces always need active state support. In some cases, like the Iceland-UK Cod wars for fishing rights in the North Atlantic, regular military force was never used.[13] Yet, it is a helpful way to understand how states

use symmetric and asymmetric capabilities in tandem to further their national interests.[14]

Coast Guards and Grey-Zone Operations

The most prominent feature of China's grey-zone tactics in East Asia is its increased use of Coast Guard vessels in coercion operations. In the East China Sea, there has since 2012 been a surge in Chinese Coast Guard presence.[15] China's vastly capable CG vessels are mostly modified naval warships that are continually deployed in the contiguous zone around the Senkakus, keeping up a regular presence in the territorial sea. Beijing's regular CCG patrols within the 12 nautical miles zone appear intended at probing a perceived seam in the U.S-Japan security treaty, where US treaty obligations can only be invoked in the event of an armed attack.

In the South China Sea too, China's growing use of non-conventional means to assert control is raising concerns among neighbouring countries. The Chinese Coast Guard has inducted two massive 12,000-tonne cutters (the Haijing 2901 and Haijing 3901), that have been intimidating and harassing the ships of other states in the South China Sea.[16][16] With a length of 165 metres (541 feet), a beam of over 20 metres (more than 65 ft), these two cutters are the world's largest coast-guard vessels and displace more than most modern naval destroyers. As China modifies its naval vessels for maritime law enforcement, many observers suspect that a proxy-naval strategy of hard-power dominance is playing out in maritime-Southeast Asia.

Expectedly, Southeast Asian powers are also beginning to use their Coast Guards to support their own territorial claims. Vietnam recently ordered two 4,000-tonne warships for its Coast Guard, with plans to flood the 'zone' with its law enforcement forces during the next standoff with China. The Philippines, Malaysia and Indonesia have likewise initiated the build-up of coastal agencies to stave off Chinese aggression.[17]

Regional states are expanding the roles of their coast guards to better come to grips with China's maritime assertiveness in the contested seas. At a time when the spectrum of maritime-related

threats—ranging from natural disasters, piracy and terrorism, to environmental pollution, illegal fishing and migration—is rapidly growing, Southeast Asian states find that they lack the scale and sophistication of capabilities needed to respond to China's aggressive moves. Even so, Hanoi's development of a state-supported fishing boat militia to hold off China at sea has been noteworthy.[18] The injunction to the country's commercial fishermen to use stronger boats and for military-trained people to prepare for a clash with Chinese militias is being taken seriously by other states in the region, even if some continue to doubt the efficacy of such measures.

The Development of China's Coast Guard

In 2017, China's coast guard had 225 ships weighing over five hundred tonnes and capable of operating offshore, and another 1,050-plus confined to closer waters, for a total of over 1,275 ships—more hulls than the coast guards of all its regional neighbours combined.[19] By 2020, the force will have an estimated total of 1,300-plus ships: 260 large vessels capable of operating offshore, many capable of operating worldwide, and another 1,050-plus smaller vessels confined to closer waters. Not only will China add 400 more coast guard ships by 2020, over 200 of these ships will be capable of operating offshore.[20]

More importantly, as China replaces its entire fleet of older and less capable large patrol ships, its coast guard is developing the capability to operate farther offshore for longer periods. China's new constabulary ships feature helicopter hangars, interceptor boats, deck guns, high-capacity water cannons and improved sea keeping. Most new coast guard vessels, like the new Coast Guard cutter 3901, have the armament of warships—76 millimetre rapid fire guns, two auxiliary guns, and even anti-aircraft machine guns. The new vessels also have high-output water cannons mounted high on their superstructure. During the HYSY-981 oil rig standoff with Vietnam in 2014, these vessels demonstrated their prowess as they damaged bridge-mounted equipment on Vietnamese vessels and forced water down their exhaust funnels.[21]

A hallmark of China's Coast Guard modernisation is the development of ships dedicated to particular missions.[22] China's massive shipbuilding industry is developing vessels that focus on designs oriented toward specific requirements. All these ships and craft remain highly capable of acting in other roles, particularly those related to promoting sovereignty in disputed South and East China Sea areas.[23] In the main, however, China's new ships play an important role in coordinating elements of China's maritime militia to ensure a highly organised campaign of harassment and coercion in the contested commons.

Grey-Zone Operations in South Asia

Even as much of the debate around 'grey-zones' surrounds Chinese irregular tactics in East Asian waters, there has been some debate over whether South Asia faces a similar threat from non-state actors in the littorals seas. Indeed, beyond violent competition between states in East Asia, the grey-zone also implicates the tension between state and non-state actors in South Asia. How actors in the grey zone break, ignore, and diminish the rules-based international order, upending the established rules of conventional conflict, can best be understood by recounting the recent experiences of the Pakistan navy.

In August 2014, the Al Qaeda staged a brazen attack on Pakistan's naval dockyard at Karachi, attempting to hijack the PNS Zulfikar, a Pakistani warship.[24]At the time, the ship was preparing to sail for the Indian Ocean to join an international flotilla. The militants, who approached the docked vessel in an inflatable boat wearing marine uniforms, had advance information about the ship's onboard security arrangements. As they approached the ship, a lone sentry onboard observed the suspicious movements and alerted security personnel. A gunfight ensued in which the attackers were subdued. To Islamabad's horror, among those that had helped Al Qaeda carry out the attack were radicalised cadres of the Pakistan Navy.[25] In the aftermath of the attack, Indian analysts considered the prospect of militant activities in India's near-seas. Could Pakistan-based non-state actors use Pakistani naval assets to launch strikes on Indian naval vessels? Or infiltrate India's maritime establishments to attack naval assets? The Karachi dockyard attack had been eerily similar

to another assault in 2011, when radicalised elements of the Pakistan navy joined forces with Al Qaeda to organise a hit on the PNS Mehran, the PN's premier naval air-station in Karachi.[26] The attack had followed failed talks between the Pakistan Navy and Al Qaeda over arrested navy personnel with suspected links to the militant organisation. It was clear to Indian watchers that the attacks on Pakistani naval bases were symptomatic of 'grey-zone' conditions where the 'rules of engagement' (ROEs) had been unclear.[27] No answers were easily forthcoming, however. Unlike the incremental strategies of Chinese militias in the South China Sea, Pakistani militant forces seemed intent on striking hard. While the absence of communication between rival forces is always a troublesome issue, the Al Qaeda's approach suggested that the possibility of a negotiated settlement simply did not exist.

There was also the big question that hung heavy in the air: Could the Indian navy sink a Pakistani war vessel being commandeered by Pakistan-based terrorist elements? In the absence of evidence that the militants have been trained, funded or sponsored by Pakistan intelligence or maritime agencies, would the Indian navy be justified in making a pre-emptive strike on a Pakistani warship? There were many questions, but neither the intelligence nor the law seemed clear about what needed to be done.[28] In the years since, India's naval planners have been preparing for situations where conventional security measures are rendered ineffective. Not only has the Indian Navy upgraded flotilla security measures in the Arabian Sea, it has also noted the need to deal with hybrid operations in the new maritime strategy document.[29] The Indian Navy's fears about hybrid attacks in ports and coastal facilities were seemingly validated when intelligence reports in July 2108 suggested that the Jaish-e-Mohammad was planning to attack Indian Navy warships using deep sea divers.[30]

Arguably, the more diabolical demonstration of the grey phenomenon in South Asia came in the form of the 26/11 attack on Mumbai.[31] In November 2008, ten heavily armed Pakistani terrorists, supported by Pakistani intelligence agencies entered India's premier coastal metropolis via the sea-route, killing 166 people and injuring over 300 in their rampage. The attacks roused the Indian maritime security establishment from its complacency,

leading to a significant strengthening of coastal security measures.

It is relevant that violent extremist organisations (VEOs) such as the Lashkar-e-Taiba (LeT) leverage the absence of government authority to carry out irregular warfare. With a permeable environment and minimal government presence, the Indian-Pakistan coast remains open to transient craft.[32] Such an environment offers myriad advantages compared to overland routes where government checkpoints and patrols are far more rigorous. Unfortunately, despite improvements, India's coastal architecture remains vulnerable from attacks by Pakistan-based VEOs. The lack of governance and increased radicalisation has in fact opened up new 'grey-spaces' in South Asia, with non-state actors ever more capable of operating in the vulnerable sub-continental littorals.

China's 'Three Warfares'

Away from Pakistan, New Delhi has also had to contend with another form of 'grey-zone' tactic that does not involve non-state actors or kinetic attacks. For the past decade, China has been actively deploying the 'three warfares' (3Ws) strategy—media, psychological and legal warfare—to weaken Indian resolve in South Asia and the Indian Ocean Region.[33] The 3Ws strategy goes beyond propaganda wars and misinformation campaigns. Expanding conventional war dynamics into the political domain, it is aimed at undermining the adversary's organisational foundations and military morale. A slow-moving and surreptitious ploy, the 3Ws are designed to subdue the enemy without ever needing to fight.

China's preferred 3Ws instrument is psychological warfare. The peacetime applications of psy-ops techniques against India involve the use of subtle coercion to influence New Delhi's decision-making calculus. The Communist party's media mouthpiece Global Times' acerbic write-ups regularly seek to shape international opinion, creating doubts, even fomenting anti-India sentiments. China also sends veiled warnings to dissuade India from military activity in territory it claims to be its own. In a maritime context, an overt example of psy-ops was the incident in

July 2011 in which a Chinese source is supposed to have issued a warning to an Indian warship, INS Airavat, operating off the coast of Vietnam.[34] China did not own up for the act but it was more than clear to all actors concerned where the warning had emanated from, who it targeted, and what it meant to convey.

Interestingly, China's 'three warfares' seems to be a modern-day version of 'unrestricted war', a military concept developed in 1999 by two Chinese colonels, who argued that war had gradually evolved to "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."[35] China's recent installation of marine observatories in the Exclusive Economic Zones of Pakistan and Maldives, for instance, clearly have a dual purpose – marine scientific research and naval surveillance, with the ultimate intention of facilitating forays by Chinese SSN and SSBNs.[36] Even so, China's 'unrestricted warfare' is seen by many as an explicit response to the US' overwhelming victory in the 1991 Gulf War.[37] The implication that modern warfare could no longer be limited to military means held true for all of China's adversaries and competitors. China's 3Ws is not meant to distinguish between soldiers and civilians; its purpose is to render society into a battlefield. Its only rule is that there are no rules; nothing is forbidden. China's 3Ws may not be classical asymmetric warfare, but the way it attempts to transcend the traditional concepts of kinetic engagement, gives it an aura of unconventional 'grey-zone' tactics. This also means that in order to combat 3Ws effectively, one needs a comprehensive approach encompassing diplomacy, information, the military, and economics.

Conclusion

The future is poised to witness an increase in hybrid warfare in Asia, as aggressive powers seek to blur the lines between military, economic, diplomatic, intelligence and criminal means to achieve political objectives. While full-scale warfare remains improbable, some powerful nations are likely to continue to exploit the 'grey-zone' between war and peace to ensure that the balance of forces continues to remain in their favour.

The lessons in the case of Southeast Asia are instructive. China, which helped nurture the grey-zone in the South China Sea, is practically ascendant, with no sign that opponents—including the United States—are willing to take on its subsidiary forces. What works for Beijing is that it has the numbers on its side, with each of China's three sea-forces possessing more ships than its presumed adversaries. Importantly, the PLAN's doctrine of operations increasingly recognises this advantage, and the domestic shipbuilding industry too is intent on capitalising on it. Numerical superiority allows China's forces to flood the maritime grey zone in ways that its neighbours, as well as the United States, may find hard to counter. Understanding this challenge confronting maritime East Asia could be a crucial first step for India in addressing its own issues in the South Asian commons. For states like India, unaccustomed to maritime grey-zone 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 for law-abiding states is to continue to work towards a 'rules-based order' in the Asian commons. At the same time, regional maritime agencies must be prepared to operate and fight in conditions of increased ambiguity, leveraging all the instruments at their disposal.[38]

Endnotes

[1] Michael Green, Cathleen Hicks, Jack Cooper, "Countering Maritime Coercion in Asia", Centre for Strategic and International Studies, Jan 2017, https://csis-prod.s3.amazonaws.com/s3fspublic/publication/170505_GreenM_CounteringCoercionAsia_Web.pdf?OnoJXfWb4A5gw_ n6G.8azgEd8zRIM4wq.

[2] Micheal John Hopkins, The Rule of Law in Crisis and Conflict Grey Zones: Regulating the Use of Force in a Global Information Environment (Routledge: London and New York), 2017, pp. 38-39.

[3] Andrew S. Erickson and Conor M. Kennedy, "China's Maritime Militia", Center for Naval Analyses, February 2016.

[4] China's militias were used to oppose the USS Lassen's sail-past the Subi Reef in 2016; See Christopher P. Cavas, "China's 'Little Blue Men' Take Navy's Place in Disputes", Defense News, November 2, 2015.

[5] "China's military is turning its aggressive South China Sea Tactics on Japan", The Business Insider, January 27, 2018.

[6] Ibid.

[7] J Mattis and F. Hoffman, "Future Warfare: The Rise of Hybrid Wars", US Proceedings Magazine 2005.

[8] Jack Cooper, Andrew Shearer, "Thinking clearly about China's layered Indo-Pacific Strategy", Bulletin of Atomic Scientists, 2017, Vol 73, No.5, pp. 307, http://milnewstbay.pbworks.com/f/Mattis FourBlockWarUSNI Nov2005.pdf.

[9] Stavridis, J, Maritime Hybrid Warfare Is Coming, Proceedings 142 (12).

[10] Robert Johnson, "Hybrid War and Its Countermeasures: A Critique of the Literature", Journal of Small Wars and Insurgencies, Volume 29, 2018 – Issue 1, https://www.tandfonline.com/doi/abs/10.1080/09592318.2018.1404770?src=recsys&journalCode=fswi20.

[11] Joshua Himes, "Iran's Two Navies- A maturing maritime strategy", Institute for the Study of War, October 2011.

[12] Andrew S. Erickson, "New Pentagon China Report Highlights the Rise of Beijing's Maritime Militia", The National Interest, June 7, 2017.

[13] Sverrir, Steinsson, "The Cod Wars: a re-analysis", Journal of European Security, Volume 25, 2016, Issue 2.

[14] "Four Chinese CG ships enter Japanese waters around Senkakus", The Japan Times, January 6, 2018.

[15] "Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response", Ministry of Foreign Affairs of Japan, January 4, 2018.

[16] "China Coast Guard's New 'Monster' Ship Completes Maiden Patrol in South China Sea", The Diplomat, May 8, 2017.

[17] Nguyen The Phuong And Truong Minh Vu, "Vietnam Coast Guard: Challenges and Prospects Of Development", Asia Maritime Transparency Initiative, January 2017.

[18] "Vietnam's Fishing 'Militia' to Defend Against China", VOA News, April 18, 2018, https://learningenglish.voanews.com/a/vietnams-fishing-militia-to-defend-against-china/4340613.html.

[19] Andrew Erickson, "Numbers Matter: China's Three 'Navies' Each Have the World's Most Ships", The National Interest, February 26, 2018.

[20] Ibid.

[21] Ibid.

[22] Ryan Martinson, “The Arming of China’s Maritime Frontier”, China Maritime Report No 2, June 2017.

[23] Ibid.

[24] “Al Qaeda Militants Tried to Seize Pakistan Navy Frigate”, The Wall Street Journal, September 16, 2014.

[25] “Al Qaeda’s Worrying Ability to Infiltrate the Pakistani Military”, The Diplomat, September 18, 2014.

[26] “Pak Navy says Air base under Control After Attack”, The Express Tribune, May 23, 2011.

[27] Discussions with senior officers and maritime experts at the National Maritime Foundation, October 2015

[28] Ibid.

[29] Ensuring Secure Seas, Indian Maritime Security Strategy, Naval Strategic Publication (NSP) 1.2, Headquarters, Ministry of Defence (Navy), October 2015, P.6, https://www.indiannavy.nic.in/sites/default/files/ Indian_Maritime_ Security_Strategy_Document_25Jan16.pdf.

[30] “Jaish Terrorists Training In Deep Sea Diving To Hit Navy Warships”, NDTV, July 18, 2018.

[31] Alan Cummings, “The Mumbai attack – Terrorism from the Sea”, Centre for International Maritime Security, July 29, 2014.

[32] Ibid.

[33] Abhijit Singh, “China’s Three Warfares and India”, Journal of Defence Studies, Volume 7, Issue 4, October 2013.

[34] “China harasses Indian naval ship on South China Sea”, The Times of India, September 2, 2011.

[35] Qiao Liang and Wang Xiangsui, “Unrestricted Warfare”, PLA Literature and Arts Publishing House, February 1999.

[36] Brahma Chellaney, “A challenging time for the Indo-Pacific”, Livemint, March 18, 2018.

[37] Nora Bensahel, "Darker Shades of Grey – Why Grey Zone conflicts will become more Frequent and Complex", Foreign Policy Research Institute, February 13 2017.

[#]The USI Journal thanks the Observer Research Foundation for permission to carry this article which was published as an ORF Special Report on 03 Aug 2018.

[@]A former naval officer, **Commander Abhijit Singh**, Senior Fellow, heads the Maritime Policy Initiative at ORF. A maritime professional with specialist and command experience in front-line Indian naval ships, he has been involved the writing of India's maritime strategy (2007). He has headed the Indian Navy's History Division in 2008 and been a Research Fellow at the MPIDSA from 2013 to 2016. His articles and commentaries have been published in leading Indian and International strategic affairs journals.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

Securing India's National Security in the Era of Grey-Zone Conflicts: Case of Cyber Warfare

Ms Poornima Balasubramanium[@]

Abstract

The international security scenario currently faces new and evolving nature of the conflict that teeters between war and peace. Tactics of grey-zone conflict have unfolded to be a major cause of concern that has left the states in limbo. The cyber domain has essentially become a fundamental tool used in such conflicts by virtue of the world being closely knit by networks controlled by cyberspace. The article assesses the kind and level of threat posed by cyber-centric grey zone conflicts to Indian national security and international stability.

Introduction

Cyber-attacks, misinformation campaigns and propaganda have

been occurring so rampantly in this era where communication and connectivity have been made digital to a larger extent. Cyber-attacks using tools such as ransomware and spyware have time and again demonstrated the damage they inflict on the target. State infrastructure and entities have of late become targets of these malicious cyber weapons. With cyberspace becoming a realm, cyber warfare will direct the nature of warfare and the characteristics that define it in the 21st century. What makes cyber warfare an issue of concern is that it falls in the grey zone between war and peace. Despite affecting state sovereignty and security (sometimes drastically), cyber warfare is not considered an act of aggression that provokes a war. While the cyber domain

has been used for its multifarious advantages, the flip side of its potential bodes much uncertainty for global and state security.

Grey Zone Conflict: Negative Peace?

Peace can either be seen as positive or negative peace. Positive peace guarantees sustainable stability and security. Negative peace warrants the absence of violence while tension and abuse continue to persist. This perspective avoids the simplistic view of peace that is built on the notion that "peace means the absence of war". Grey-zone conflict is an embodiment of the concept of negative peace. State and non-state actors use instruments such as political warfare, economic warfare, information warfare, cyber warfare among many others, in their conflict against their opponent without the involvement of armed violence. Meddling in the election process of another state to alter the outcome, imposing sanctions and trade curbs, propagating fake news that can be detrimental to a state's public image are some of the means through which conflict in the grey zone has been evolving. Grey-zone conflict can be defined as: "The process of conflict-induced change is known as grey-zone conflict, in which states conduct operations that only occasionally pass the threshold of war."[1] The impact is profound but just not enough to pass *Jus ad bellum,* the criteria to be considered before waging a war. The concept of *Jus ad bellum* was introduced in International Law during an era when only conventional tactics of warfare were mostly practised and posed critical security risks to international security. With the evolution of the nature of warfare, the loopholes in the laws governing warfare have been widening. This very lacunae in international law, which does not address facets of grey-zone conflict, is being exploited by state and non-state actors. Donning a double-edged sword, cyberspace is a capable means of grey-zone conflict. Its dynamic nature needs to be appraised to gain a better perspective of the threats it poses to state security.

The Vagaries of Cyber Warfare

In today's world, technology is power. At the same time, information is also power. Whosoever controls these can effectively exercise power over the international system.

Cyberspace uses technology that disseminates information from one end of the globe to another. Advances in the Industrial Revolution 4.0 such as robotics, artificial intelligence, and cloud computing — with every digital service steered by the Internet of Things — have further opened new avenues to manoeuvre cyberspace, giving it the key to potentially penetrate the structures of society.

Cyber Threats to Critical Infrastructure

The network of Critical Information Infrastructure (CII), which ensures that the functioning of a state is carried forward, is mainly connected through cyberspace. The security of the CII is of paramount importance for the state as its national security hinges on these infrastructures to a greater degree. A disruption caused in the network even for a short period could cause chaos as it can impede services such as transportation, communication, and power. The CII in any state is protected by multiple layers of physical safeguard protocols. However, since these infrastructures are inter-linked in cyberspace to connect to a central command, they are rendered vulnerable to cyberattacks. Several attempts have been made to attack the CII of states. Most of these attacks are identified post execution when considerable disruption has already been caused. Tracing the origin of these attacks is also a task for which not many states are equipped.

Highly sophisticated cyber technologies like malware and spyware can be deployed on any Programmable Logic Controller (PLC) device and once installed, they can reprogram and command the entire system.[2] States have been at the receiving end of threats such as data mining traps, sabotage campaigns, cyber espionage that have been frequently endangering their security. Yet, these kinds of attacks do not attract physical retaliation because of their asymmetry and covert nature. Reports show that states like the US, China, Russia, Israel and Iran have been using the cyber domain, both for their offensive and defensive operations in the grey zone.[3] Miriam Howe, a Cyber Security Consultant at BAE Systems, opines: “A characteristic of the grey zone is the inherent uncertainty and deniability of operations in cyberspace- the ability to remain covert, difficulties in attribution, false flags and deception often means the absence of

a smoking gun".[4] The capability of cyberspace in grey-zone conflicts and of it being unpredictable but crippling has been demonstrated a number of times in the recent past.

- **The Stuxnet:** The Stuxnet worm was a product of the US-Israel collaboration to develop a weapon to disrupt Iran's nuclear program without the use of conventional forces. The idea developed in the early 2000s and "Operation Out of Box" was executed in 2010 on the Iranian nuclear enrichment facility in the Natanz region.[5] Cyberweapons work with a similar concept as a conventional missile. They consist of two parts: the delivery system and the payload. In a cyber weapon, the delivery system delivers and distributes the code or the cyber payload to the target system. The code (payload) then infiltrates the system and reprograms it, steals, and transfers data and also destructs the system.[6] The Stuxnet worm is deduced to have probably infected the computer system through an "infected USB" (the delivery system). After getting inside the system, the worm (cyber payload) got access to the control system of the centrifuges of the nuclear reactors. After gaining control, the worm re-programmed the centrifuges. It executed two different patterns of attacks for several months together. One, it drastically increased the speed of the centrifuges for 15 minutes and set it back to the normal speed. After a month or so, it reduced the speed of the centrifuges down to 50 minutes. The erratic speed patterns caused the centrifuges to disintegrate, and it brought the need for 20% of the reactors to be decommissioned. Within months, the Stuxnet could infiltrate into a "supposedly" air-gapped control system of a nuclear plant and delayed the progress of the program.[7] Stuxnet is the first known worm to "target and infiltrate industrial Supervisory Control And Data Acquisition (SCADA), a software that is used to run chemical plants as well as electric power plants and transmission systems."[8] Owing to its covert and uncertain nature, it took almost a few years for Iran to identify the malware and its place of origin. The ambiguity in the character of the attack failed to testify whether the attack tantamounted to an act of aggression

under *Jus ad bellum,* although it violated Iran's sovereignty and revealed the vulnerability of the state.

- **BlackEnergy 3:** In 2015, the Ukrainian Power Grid came under a cyber-attack. The outage plugged the eyes of nearly 30 substations and left 2,30,000 citizens in darkness and cold as the electricity that powered the lights and heaters was cut off through a few mouse clicks. Hackers sitting elsewhere were able to control the cursor in an operating system in the main station that allowed a program to be activated in the system, eventually shutting down the electricity. Further, they were able to sever the backup power supply of two power distribution centres. In few weeks, the hackers had managed to trap the systems through spear-phishing and gained backdoor entry into them. The control systems of the power grid were supposed to be much more secured than the systems in the US but unfortunately, they fell short of securing the system enough to have a resistant SCADA network, which was remotely penetrated with ease.[9] The attack was reported to be orchestrated by Russia with the support of criminal networks against Ukraine as part of the long-drawn conflict between both states. The infamous Russian hybrid warfare strategies also incorporate grey-zone cyber warfare tactics.

Cyber-Information Warfare

Cyberspace has been proficient enough to propel misinformation campaigns that could influence the thoughts and opinions of people. Misdirecting narratives can impact the political and social stability of the states. Fake news and propaganda are being circulated on social media platforms and unfortunately sometimes, even in mainstream media. The erroneous generation and promotion of uncontrolled and unvetted news have affected society's thought process making them susceptible to the cons of the post-truth era.

Information warfare is indeed a threat to the interests of states as domestic and international opinion matters much for states' impression and stature in the international community. Nevertheless, states have been unable to confront cyber-information warfare in its entirety because of the ubiquitous nature

of cyberspace. This issue demands to be tackled by the erudite employment of public diplomacy, awareness campaigns and other defensive methods and not by violent retaliation. Such is the nature of the grey-zone conflicts.

A Bird's Eye View into the Indian Scenario

As emphasised before, grey-zone conflicts have changed the notion of warfare and have now become an indispensable aspect of the conflict between and among state and non-state actors. India, like any other fast-developing state, encounters this threat. This is partly due to the dicey geopolitical environment it is a part of. India has been facing thrice the average number of cyberattacks that are affecting the world. A lot of these have been found to have their source in Pakistan and China.

The attempted attack on the control systems of the Kudankulam Nuclear Power Plant in the state of Tamil Nadu in 2019 is a classic example. The DTRACK malware penetrated the administrative computer of the plant and had taken information stored in the system. Although in this case only the administrative system was targeted, there were possibilities of a control system being attacked like in the case of Stuxnet. The ramification would have been detrimental as a nuclear leak could have harmed the people and the environment. The psychological impact of the Kudankulam attack had mobilised political parties and activist to call for the shutting down of the Plant, which would have a drastic impact on India's energy needs in the future.[10] Though the attack was attributed to a North Korean company, Lazarus Group, connections to any state actor was not established.

The Cyberthreat World-time Map reports that India is the seventh most attacked state in the cyber realm. According to the Indian National Security Council Secretariat report of 2018, 35% of India's cyberattacks are of Chinese origin. Though high-impact attacks targeting CII have not taken place, there have been constant attempts at espionage and theft of sensitive data from government and private enterprises. One report even accused China of using the Stuxnet worm to disrupt India's communication satellite.[11]

For a major power like India, threats from states, especially its neighbours and the non-state actors they support, are a plethora. More so, Pakistan has been relying on cyber warfare as one of the efficient tools that would, on one hand, disrupt the functioning of the state and on the other, not escalate the conflict. Apart from this, the rounds that fake news and propaganda materials originating from Pakistan have caused a deep dent in Indian politics and society, furthering the divide between people. Many shreds of evidence have been provided that proves the involvement of external sources in funding and proliferating such influence campaigns that work against the state. Social network platforms have been used prevalently for this purpose where different cyber tools enable the circulation of these messages that it reached every corner of social media. Following is a small excerpt of one such incident:-

> "The 2013 riots in Muzaffarnagar (UP) were aggravated by the use of social media networks by suspected terror groups. On 21 November 2013, the then Home Minister Sushil Kumar Shinde had observed, "More recently, the Muzaffarnagar riots were fanned by similar misuse (of social media)." There is mounting evidence that the abuse of the Internet against India is substantially orchestrated under the aegis of Pakistan's external Intelligence agency, the Inter-Services Intelligence (ISI). A classified note of a high-level security review meeting held in New Delhi in September 2012, noted, "The ISI is now working on a bigger game-plan in training terrorists in the use of cyber and computer technology as the Pakistani agency feels India is not fully equipped in dealing with incidents of cyberwar or attack." Importantly, the note observed, the training is given to subversive elements by ISI's cyber experts played a key role in spreading hate campaigns through MMS and SMS, targeting people from the Northeast in the wake of ethnic violence in Assam. The note warned that this trend would only increase in days to come, and this was also the reason why ISI was increasingly stressing the recruitment of more educated youth by Islamist terrorist formations. An unnamed Indian intelligence officer stated, further, "It is almost certain that the Pakistani agency was behind the recent cyberattack

> on India, at least indirectly. Having tasted success, they will try it again in future and on a much bigger scale. So, we must be prepared to deal with this challenge."[12]

After the abrogation of Article 370 from the constitution of India, a surge in the volume of cyberattacks was observed from Pakistan, with several fake accounts that were created to swiftly circulate fake news, videos, and morphed photographs to instigate unrest in Indian society. The cyber domain has been a tool for Pakistan for its psychological operations against India, to shape the opinion of the people in both the states and worldwide. Such information warfare could tarnish India's image and credibility at the domestic as well as international level. Challenges to India's diplomatic manoeuvrability have arisen out of misperceptions and deceptive information that is propagated through social networking platforms. Cyberspace has been immensely used to bolster propaganda by manipulating algorithms and DDoS capabilities.[13] Though India has been largely successful in overcoming the war of narratives with Pakistan, it leaves behind stains that can hamper India's national interests, thanks to the grey-zone nature of cyberspace.

The Way Ahead

The absence of international norms and laws that adequately govern the manifestations of grey-zone conflicts, especially cyber warfare, has the potential to extremely affecting state security. More so, in a complexly interdependent world that makes wars costlier, states will increasingly invest in capabilities that help them in grey-zone conflicts. Cyberspace will be a conducive battlefield towards that end. Irrespective of the defensive capabilities a state possesses, the uncertainty that cyber warfare produces in the grey zone will be a hard challenge to confront in the future. The threat has already started to loom, and it is important that states, including India, need to be aware of the intricacies of conflicts of such kind. States need to come together to be aware of the nature of such threats as well as cooperate to bring about institutions and regimes that bring clarity by removing the greyness of this zone and build confidence among the states. Collective action can bear fruit, apart from securing one's national security, in keeping the threat under control.

Over the years, India has been building its defence against cyber warfare by instituting various laws, organisations, and regulations as part of its digital revolution. India has also been in active collaboration with states like the United States and Israel to share best practices and participate in joint training initiatives to fortify itself in the cyber domain. Despite these measures, cyberattacks have been a grave threat for India. The National Cyber Security Strategy is a good head start. It aims at bolstering India's overall cyber defence capabilities that will equip the state to be resilient in cyberspace. However, effective implementation of the strategy is imperative, which demands the investment of resources including finance as well as human capital. India must also counter the narratives that are mobilized against it, especially during sensitive times such as now, during the pandemic. This can be done mainly through connecting with its people and those abroad and raising awareness about the grey-zone threat. The mainstream media, for instance, can keep people informed about the dangers of fake news and help them build resilience towards such peril. In this conflict, the general public is the first line of battle. A resilient society will eventually show zero porosity for disinformation.

Conclusion

Cyber warfare and cyber-information warfare portend an era where the deniability of such means of warfare can be used by state and non-state actors against their targets while leaving the conflict in the grey zone. The ramifications of such assaults can be irreversible or at the least, extremely hard to recover from as they target high-value national assets including the CII as well as information, the new-age oil. Advancements in technology can lead to mutation and thereby, to the evolution of the nature of the grey-zone conflict. Such advancements can simultaneously be used to develop defensive walls that can preserve the security of a state as well as the international system. The hazards of cyber warfare in the grey zone linger even as the Covid-19 crisis has kept the world reeling. At this crucial juncture, India must not lower its guard and prepare to face the future of warfare in the grey zone as it treads the path in its pursuit of power and progress.

Endnotes

[1] David Carment and Dani Belo, “War’s Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare”, *Canadian Global Affairs Institute,* Policy Paper (2018).

[2] Robert Mcmillan, “Was Stuxnet Built to Attack Iran’s Nuclear Program?”, *IDG News Service* (Boston), September 21, 2010, https://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

[3] Abhijit Ahaskar, “How Cyberattacks Are Being Used by States Against Each Other”, *LiveMint,* June 21, 2019, https://www.livemint.com/technology/tech-news/how-cyberattacks-are-being-used-by-states-against-each-other-1561100711834.html.

[4] “Competition and Conflict in the Grey Zone: Government Insights”, BAE Systems, accessed 15 June, 2021, https://www.baesystems.com/en/cybersecurity/feature/competition-and-conflict-in-the-grey-zone.

[5] Nicole Perlroth, “Researchers Find Clues in Malware”, *The New York Times,* May 30, 2012, https://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

[6] Kartik Bommakanti, “The Impact of Cyber Weapons on Nuclear Deterrence: A Conceptual and Empirical Overview”, *ORF Issue Brief,* n. 266, 2018.

[7] “How Stuxnet Attacked a Nuclear Plant,” BBC, accessed June 15, 2021, https://www.bbc.com/timelines/zc6fbk7.

[8] Mark Clayton, “The Stuxnet Malware Is Weapon Out to Destroy Iran’s Bushehr Nuclear Plant?”, *CS Monitor,* September 21, 2010, see website https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

[9] Jose A. Bernat, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, *Wired,* March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[10] Stephanie Findlay, “India Confirms Cyber Attack on Nuclear Power Plants”, *Financial Times,* October 31, 2019, https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6.

[11] Elizabeth Radziszewski, Brendan Hanson and Salman Khalid, “India’s Response to China’s Cyber Attacks post- Kashmir Decision”, *LiveMint,* August 19, 2019, https://www.livemint.com/news/india/india-sees-dramatic-rise-in-cyber-attacks-post-kashmir-decision-1566217795883.html.

[12] Sanchita Bhattacharya, “Cyber Wars”, *Outlook,* November 20, 2014, https://www.outlookindia.com/website/story/cyber-wars/292633.

[13] Shashank Shekar, “Pakistan Bots Wage Cyber Warfare”, *msn,* August 12, 2019, https://www.msn.com/en-in/news/newsindia/pakistan-bots-wage-cyber-warfa/re/ar-AAFHyyy.

@**Ms Poornima Balasubramanium** is a PhD research scholar at the Department of Geopolitics and International Relations, Manipal Academy of Higher Education, India. Her research interests include Conflict analysis, Indian Foreign Policy and National Security, Geopolitics of West Asia.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

The Corona Whodunit: Grotesque from the Grey Zone*

Group Captain (Dr) K Ganesh (Retd)[@]

Abstract

SARS-CoV-2 is not a Weapon of Mass Destruction (WMD) for China, but it does offer a range of options in future Grey Zone wars. Biological weapons in conventional wars in the modern-day world offer few tactical uses because of the comparatively long gestation period. However, they offer a perfect deniable weapon to debilitate economies and populations as the experience with Covid has shown. The pandemic has already spurred conflicts within countries and societies to the dream extent of militarists who see, in the event, an opportunity to weaken their opponents.

Introduction

The Grey Zone is synonymous with 'The Twilight Zone', a phenomenally successful American television series presented by Rod Serling over five seasons from 1959 to 1964. The show was a combination of science fiction, paranormal, fantasy and horror. Each episode was an independent story dealing with strange and unusual events, an experience described as entering 'the Twilight Zone', and often with a surprise ending and a moral.

The modern term 'disruptive technologies' when applied to the military field refers to those technologies which transform an existing way of war fighting, or in other words bypasses that way. In the same sense, Grey Zone war bypasses familiar or codified ways of war to secure an advantage which may be in the tactical to strategic fields. Examples of Grey Zone war abound right from our epics. In the way of how things evolved, we can offer a

perspective of Grey Zone that is uniquely Indian. *Hiranyakashipu* was the first to prepare for the transitory phase of neither here nor there, as a ruler, seeking a set of clauses where his own conventional and asymmetric capabilities would not get overwhelmed.[1] This led to his denouement at the hands of *Narasimha* who was neither man nor animal, by his bare hands, without weapons, at twilight dusk, which was neither day nor night, on the footsteps of his palace, which was neither indoor nor outdoor, on the lap of the man-lion, which was neither on earth nor in the sky.

In the later human avatars of *Vishnu,* you can see in conflicts, fought in Indian epics, the play of this element of grey in how *Vali* is slain, in how *Indrajit* is slain, in how *Duryodhana* is laid low, in how *Brihannala* defeats the *Kaurava* Phalanx of *Maharathis,* or how *Shikhandi* screens *Bhishma* as a target for Arjuna.[2] There were not just greys of gender, camouflage and strategy but even moral codes of war, commonly accepted and respected. They were clear grey stratagems which we are now calling Grey Zone war.

This pandemic, that is still unfolding before us, offers many shades of Grey/Twilight that scientists and analysts are still struggling a year and more later to get a feel for it. Many theories abound about the virus being the by-product of Chinese experiments to produce a weapon with devastating effects and deniability for use in Grey Zone war. This article comments upon this thesis.

The Conspiracy Theory

It must be the most bizarre idea which, over the days and months, got into textured layering and nuance that we are now witness to what can be called the acknowledging of the plausible. The origin of this SARS-CoV-2 has been a humdinger! In a normal course of our human experience, we could have seen the Spanish Flu, our last experience with a flu virus that ravaged the earth as the immediate precedence. For the name itself reveals how the origins of that one was sought to be initially deflected and denied, and no guesses here, for it was the USA that obfuscated the origins of the last viral devastation to visit humanity, the exact

charge that now USA has joined others in levelling against China with President Biden ordering his intelligence officials with a 90 day window to close this argument in a decisive way. Did the Coronavirus emerge from Wuhan's lab?

Before delving into it further, let us be clear that this SARS-CoV-2 is not a Weapon of Mass Destruction (WMD). For China, the order of this probe led to her official spokesperson to contrast it with the last time Pentagon hunted for something, and informed the world about the 'WMDs of Saddam Hussein' which led eventually to a wild goose chase and the totally unnecessary war in the Middle East, a war that USA could have easily fought and cleaned up the Taliban once and for all. Instead, the Pentagon's famed intelligence had the US bark up the wrong tree, as was evident after the war was over. It shattered the international reputation of General Colin Powell as a person, and interlocutor, and US went into a rabbit hole that ended finally when the Inspector General released a damning report, and now the US is pulling out leaving behind a mess in Afghanistan. One would not be wrong to say that a US undistracted from Iraq would have focused much earlier on China, not having a changed Chinese posture and a global pandemic with its supply chain shocks to nudge it to reboot her strategic stakes.

So from where this comes, the Chinese have a point. Why would they now trust Biden's Intelligence Report? Yet, looking at how the 46th POTUS has literally placed his predecessors on the cross hairs as he deftly unknots one issue after another open, one is sanguine that President Joe Biden will leave this clearly settled once and for all. May be to ensure that his own elites and analysts do not waste their energies on another wild goose chase. So, it is Biden's unstated aim to disprove all the controversies and conspiracy theories that now surround the SARS-CoV-2 origin story.

An Analysis

In an ideal world of science, this pandemic should have had several false starts; when from some host to intermediary host to humans that bug must have jumped and fallen back, improving its code, tempering its spike protein sequences to come up

eventually as the now recognised genomic sequence of the Wuhan strain. In nature, such a thing could have happened in ideal settings where host-intermediary-human were in proximity over several months, where the virus, passing through each living organism as bat-pangolin-human, emerged with the perfect strand of Ribonucleic acid (RNA) that became SARS-CoV-2. What we do not have is record from the Chinese of these incidences of zoonotic infections; like how they recently announced a 41-year-old male resident of Zhenjiang, who was hospitalised on 28 April 2021, diagnosed as a H10N3 case of influenza of avian origin on 28 May 2021 and discharged a few days later. This is not one gap, there are several others, for here the human zoonotic phase would have involved several such cross infections before what epidemiologists call 'case zero', where the first human would have received the perfected viral strain which then jumped from human to another human.

There is equally the possibility that Dr Shi Zhengli, the top virologist who heads the Centre for Emerging Diseases at the Wuhan Institute of Virology[3] is aware of certain facts which she has been economical about. We know the World Health Organisation (WHO) initially advised wrongly about human-to-human transmission after the Wuhan outbreak[4] became an International Outbreak of concern before being officially declared as a pandemic. We also know that initially many scientists globally thought the virus spread through only droplets but the experience from several cruise liners was to suggest that it was a surface contaminant too. We know now that aerosol happens, surface contaminant is not a route for infection.[5] Dr Goldman, a microbiologist at Rutgers New Jersey Medical School, found that SARS-CoV-2 rarely passed on that way for various reasons and his findings were published in Lancet Infectious Diseases in July 2020! Yet, no real effort has been made to unearth the reasons why the Chinese and the WHO allowed the world to be misled initially.[6]

The Chinese Puzzle. We know that China tried to deny its own Wuhan medical fraternity about this novel coronavirus including how it ill-treated the ophthalmologist who opened the eyes of the world through Chinese social media to the true horrors of this

pandemic - Dr Li Wenliang![7] So two things make China take a bad place and convert it into a swamp — its initial denial about this now becoming a pandemic possibility — and its treatment of its own home-grown medical professionals who rang warning bells in Wuhan about this. Dr Shi maintained her Sphinx-like stance, unwilling to engage with her scientific community peers even.[8] When Wuhan had the laboratory infrastructure, when Wuhan was the place where case zero and the epidemic outbreak happened, why did a Virology Centre from Shanghai code the genome of the novel coronavirus (Fudan University)[9]? So from these early responses of the Chinese, we could clearly see that Chinese had more to conceal than to reveal. Could this be a coronavirus their Wuhan lab was dabbling with for scientific research purposes, one that accidentally obtained a human host? A laboratory scientist, or group of scientists, then became the group from where case zero emerged? Will China reveal Wuhan laboratory personnel's health records? Will US be able to obtain it? For, this would be the only way we can bury this ghost of it being a virus associated with a laboratory, one that emerged from serious lapses in a Bio Hazard Level 4 laboratory, where its human workers interacted with wild zoonotic viruses being studied that were bat in origin and due to proximity and leaks in protocols, the viruses were to treat their human handlers as intermediary and perfect themselves before latching on to one of them as human host? So, did the coronavirus jump from Petri dish to human?

Why one would wish to rule out the SARS-CoV-2 as a bioweapon is because it does not meet the basic qualities that scientists and military experts seek in a bioweapon.[10] The main issue is how unpredictable this novel coronavirus has been. It has shown very selective evidence so far of being a 'super spreader'; it needs certain conditions, that are still being studied, which need to be met for the virus to infect more than one person from one encounter with a host. For both outdoor and indoor events, the factors are the proverbial Swiss cheese model where the holes often do not match at all! That is one main reason why, in all probability, epidemiologists who favoured the natural herd immunity theory failed glaringly, because the virus appears to not run through populations the way it possibly could. That is also why, in actual ground situation, there are many unaffected by

SARS-CoV-2 for whom this is just one big hoax, while the unfortunate few who suffered it will remain haunted by it equally! So suffice to say, no military general worth his salt will accept such a bioweapon, one that is uncontrolled in its behaviour, in its infectivity, virulence, its incubation period, transmissibility, stability, and lethality. Just take the Indian variant studied which is called 1.617. This was weeks ago and now we see that it is 1.617.2 and 1.617.1 christened after Greek alphabet as delta and kappa respectively by WHO's new nomenclature for variants of concern, after sensitivities arose over taking the place of origin of variants to refer to them. Technically, 1.617 is the variant; the 1 and 2 are sub variants of this variant but now notified as individually of equal concern with unique characteristics. The amounts of variants, and the half a dozen concern causing ones, in the past one year have shown what we can only ascribe as natural properties of RNA viruses as they drift and shift with infections through natural pools of living organisms. While many dismissed Russian vaccine efforts for cats that appear to suffer SARS-CoV-2 from us humans, though with no serious consequences, the probability of our cats becoming reservoirs and then recycling the virus from them to us cannot be ruled out, so I would not say the Russian efforts are a wild goose chase. It reinforces the theory that this novel coronavirus is a natural one and not human engineered. However, that being said, there is also the case that without Case Zero, without health records from Wuhan's Institute of Virology, without an epidemiological map of the outbreak in Wuhan, it will never be absolutely sure that Chinese virologists had no role in this pandemic.

One wishes that the Chinese Communist Party (CCP) Politburo understands why it is in China's interests to part with all this information. Because this is not the last pandemic, with climate change on anvil, with clear challenges ahead, the chances of Chinese wet markets offering inter species jump for viruses as zoonotic or exotic to be the vehicle for a future pandemic is obvious. This scientific reality is why Wuhan got international support for its virology centre in the first place? It is also why Taiwanese scientists are always nervously monitoring new fevers or rashes across the mainland. Can President Biden squeeze from President Xi this clear evidence that we need? Can we allow

China to suffer sanctions in microbiology and virology to enforce this or will that boomerang by creating a bamboo curtain that will blind us completely to future outbreaks?

Conclusion

From Spanish Flu to SARS-CoV-2 pandemic, the biggest difference has clearly been science. Advances that made us model, predict, test, trace, and treat, even without specific biologics and antiviral agents in our armoury, have largely reduced the footprint of this bug in mortality and morbidity. If our response had been more mature, one may have saved more than 60 per cent of the casualties we have now suffered. Our candidate vaccines for COVID-19 are a clear success. It is sure that we will come up with treatments that would reverse the changes that make Covid Pneumonia or Covid end organ damage through blood clotting such killers. We will also learn to deal with other physiological disturbances and other end arterial and tissue damages.

It is clear that no matter how advanced we have emerged, we are nowhere near mimicking Mother Nature and conjuring such a predatory pathogen as SARS-CoV-2! However, it is a threat which lies in the realm of Grey Zone war.

The pandemic has already spurred conflicts within countries and societies to the dream extent of militarists who plan psychological operations (PsyOps). If you see USA, it is swords drawn between Red States versus Blue States, what with Anti Vaxxers, QAnon and other fringe groups rallying to deny various scientific aspects of this pandemic as conspiracies. China itself underwent great pain as she suffered market trust and logistics integrity, which has given rise to decoupling programs from Japan, Taiwan, Korea, and USA amongst others. If one can look at this pandemic as a daisy cutter that unsettled every presumption of geopolitics then one can be in awe of Grey Zone possibilities in the future, offered by biological agents to players among their range of options. In fact, looking at Southeast Asia and China as populations where wet markets, wild or undomesticated animal flesh is cooked at the dining table, without processing procedures of Western Meat Factories, one can wager that these regions offer

an ideal setting screen for a biological foray for weaponising a zoonotic bug and setting it upon an unsuspecting population with perfectly plausible deniability. It would be a temptation for any international strategist in aiming to disable coastal China, or for that matter in the larger Asiatic Rim to cripple any island or peninsular population, before gaming troop movements under Humanitarian Assistance and Disaster Relief (HADR) guise to temporarily occupy such vantage territory. Quad, First Island Chain Nations and People's Liberation Army (PLA) planners must be already seized of this prospect and will invest in such potential inevitably going forward! The bug will not be transient buzz; it will forever now be a bugging concern for all manner of strategists and futurists!

Lastly, for those that must keep the peace in the Grey Zone war environment, it would do much good if the unknown unknowns of the Grey Zone are dealt with not with paranoia but prescience. Prescience is a judicious mix of imagination, anticipation, and inspiration. At Kurukshetra, *Krishna* using the solar eclipse to spot *Jayadratha* to enable *Arjuna* to slay him is example of prescience[11] *as much as the dash of India's Finest which is being commemorated this year as the golden jubilee of a military feat that has no parallel in the annals of modern warfare — the Surrender at Dacca!*

Endnotes

[1] In the Vishnu Purana , Hiranyakashipu was a demon king who got a boon from the Gods which stipulated that he could not be killed by an animal or a human, by day or by night, by no weapon, neither in his house or outside it and neither in the air or on ground.

[2] Details of all these are available on the internet for those unfamiliar with Indian epics and mythology.

[3] David Cranoski, "Inside the Chinese lab poised to study world's most dangerous pathogens", *Nature,* Feb 23, 2017. Inside the Chinese lab poised to study world's most dangerous pathogens | Nature

[4] WHO (On Twitter) World Health Organization (WHO) on Twitter: "Preliminary investigations conducted by the Chinese authorities have found no clear evidence of human-to-human transmission of the novel

#coronavirus (2019-nCoV) identified in #Wuhan, #China????. https://t.co/Fnl5P877VG" / Twitter

[5] Dyani Lewis, “COVID-19 rarely spreads through surfaces. So why are we still deep cleaning?”. Nature, Jan 29, 2021. COVID-19 rarely spreads through surfaces. So why are we still deep cleaning? (nature.com)

[6] Barnani Chakriborthy, Mar 20, 2020, Fox News, China's relationship with WHO chief in wake of coronavirus outbreak under the microscope | Fox News

[7] Ken Jin Lee “Coronavirus kills Chinese whistleblower ophthalmologist - American Academy of Ophthalmology (aao.org)

[8] The Wire. Wuhan Scientist Rules Out Theories That Novel Coronavirus Originated in Lab - The Wire Science

[9] Lisa Scherring, “China releases genetic data on new coronavirus, now deadly”. Jan 11, 2020.CIDRAP, University of Minnesota, https://www.cidrap. umn.edu/news-perspective/2020/01/china-releases-genetic-data-new-coronavirus-now-deadly

[10] NATO Handbook On The Medical Aspects Of NBC Defensive Operations. Amedp-6(B). FM 8-9 Part II/Chptr 1 Introduction (fas.org)

[11] In the epic, The Mahabharata, Jayadratha, the king of Sindhu Desa (Indus Valley) killed Abimanyu, son of Arjuna on the 13th day of the war. Arjuna was furious and vowed to kill Jayadratha before sunset the next day or failing that, to kill himself. The whole Kaurava army gave Jayadratha full protection to insure Arjuna’s death. When the sun appeared to set, Jayadratha poked his head out to show that he was victorious. Suddenly the sun reappeared in the sky and Arjuna shot Jayadratha down. The story goes that Krishna hid the sun. Actually, Krishna tricked Jayadratha with the knowledge of the solar eclipse happening on that day. This was Grey Zone War in that age. The moral imperative of subterfuge is a grey subject.

* This article has been derived from Indiarubberman.com from a post titled ‘WMD: The Corona Whodunnit?” dated 02 Jun 2021 at https://indiarubbermancom.home.blog/2021/06/02/wmd-the-corona-whodunit/

@**Group Captain (Dr) K Ganesh (Retd)** is from the Army Medical Corps. He is a analyst of social, strategic and political affairs and runs two very incisive blog sites https://indiarubbermancom.home.blog and https://otherfeetotherfeatnet.home.blog

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

Grey Zone Conflict and Legal Derision

Wing Commander UC Jha (Retd)[@]

Abstract

The Grey Zone conflict falls between the war and peace on the war-peace continuum. The Grey Zone is characterised by intense political, economic, informational, and military show of force. Grey Zone actions are not new. Examples of Grey Zone tactics include cyber warfare, deception, proxy war, economic pressure, digital propaganda, and drones etc. They may also involve military show of force or intimidation and unconventional military operations. The ambiguous nature of Grey Zone activity coupled with a lack well-defined international law makes it difficult to hold Grey Zone actors accountable for their misdeeds. The United Nations, the largest international player to facilitate conflict management by states, remains an ineffective organ for conflict de-escalation in Grey Zone conflicts. There is an urgent need to upgrade international legal frameworks and mechanisms of conflict management which could be employed to address the Grey Zone conflicts.

Introduction

If a state is engaged in an armed conflict, it is said that the state is at war. If the state is not in an armed conflict, it is at peace. 'Grey Zone' is the space between war and peace involving coercive actions that do not reach the level of armed conflict. Today there are several Grey-Zone conflicts involving confrontations over territory, sovereignty and economic interests. The operations launched by Russia against Ukraine in 2014, the Russian interference in the 2016 US Presidential election[1], the Chinese interventions in the South China Sea and

intrusion in Ladakh, and Pakistan's proxy war in Jammu and Kashmir could be termed grey-zone activities. Another recent example of this kind is the killing of the Islamic Revolutionary Guard Corps (IRGC) Quds Force chief Qasim Soleimani by a US drone strike in Iraq in January 2020. In such situations, the use of military forces falls short of actual war but cannot qualify as peace.

A few states are using non-state actors and unconventional tools to destabilise their adversaries. Russian Army General Gerasimov, without explicitly using the term Grey Zone, has expressed the view that "A perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war".[2]

The laws of war or international humanitarian law (IHL) regulates relations between states by limiting the use of violence in armed conflicts.[3] IHL applies only to international armed conflict or internal armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence. International law does not clearly set out acceptable norms in many areas of the Grey Zone. The main reason is that Grey-Zone conflicts do not reach the level of an armed conflict. Besides discussing the concept of Grey-Zone conflict, this article discusses some relevant legal issues such as the effectiveness of the United Nations Charter and the means and methods of warfare that may be exploited in a Grey-Zone conflict.

Defining Grey Zone Conflict

Grey Zone has been defined by one author as, "Those covert or illegal activities of non-traditional statecraft that are below the threshold of armed organised violence; including disruption of order, political subversion of government or non-governmental organisations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage.[4] The US Special Operations Command (SOCOM) uses the following definition of Grey-Zone conflict: "Grey Zone challenges are defined as competitive interaction among and within state and non-state actors that fall between the

traditional war and peace duality. They are characterised by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks".[5]

The important characteristics of Grey Zone conflict are: (i) It remains below the threshold that would justify a military response with an aim to avoid major clashes, or attributable violations of international law; (ii) It unfolds gradually over time rather than involving bold, all-encompassing actions to achieve objectives in one step; (iii) There is lack of attributability with an aim to disguise its role at least to some extent by using disinformation or/and cyber-attacks; (iv) There is extensive legal and political justifications, often grounded in historical claims supported with documentation; (v) It stops short of threatening the defender's vital or existential interests; (vi) It is typically built around non-military tools, as part of the general approach of remaining below key thresholds for response; (vii) It may use the threat of more violent military actions; and (viii) It puts the defender in situations where strong responses appear non-viable or counterproductive, for strategic and domestic political reasons.[6]

Grey-Zone warfare has been referred to as irregular warfare, political warfare, asymmetric warfare, and unconventional warfare.[7] Grey-Zone tactics may include cyber-attacks, deception, sabotage, proxy war, assassinations, espionage, economic pressure, terrorism, and exploitation of gaps and ambiguities in the law. Manipulation of public opinion at home and abroad by using information warfare and disseminating "fake news" is an important means of creating confusion and skepticism.[8]

Grey Zone Conflicts and Hybrid Warfare

Grey-Zone conflict and hybrid war are two different concepts. The use of the term 'conflict' for the former and 'war' for the latter is intentional. However, hybrid warfare techniques may be used in a Grey-Zone conflict. In a Grey-Zone conflict, conventional military operations may be used alongside non-conventional tactics, whereas in hybrid warfare, conventional military operations are dominant and non-conventional operations are used as auxiliary tactics. Protracted engagement is one of the dominant characteristics of a Grey-Zone conflict, whereas engagements are

of short duration in hybrid warfare.[9] Parties engaged in Grey-Zone conflicts use unconventional hybrid warfare tactics such as political and information warfare, propaganda appealing to transnational actors, equipment and training of non-state actors, state-level economic pressures and unconventional operations by the security forces.

Grey Zone Conflict and the UN Charter

The UN Charter prohibits aggression. Article 2(4) of the Charter states that, "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations". Unlawful uses of force that violate provisions of Article 2(4) generally require forces engaging in military activities whether traditional armed forces or non-state armed groups. In practice, Grey Zone conflict measures are designed to avoid being identified as clear violations of the Charter even when they do constitute an unlawful use of force. A number of tactics used in Grey Zone conflict are not accounted for by the Charter's prohibition on the use of force. For example, economic measures, cyber operations, disinformation, and lawfare traditionally do not violate Charter Article 2(4). In theory, the UN Charter's prohibition on the use of force is sufficient to account for Grey Zone tactics when they resemble traditional military activities. However, when a state employs cyber capabilities in a Grey Zone conflict to damage or disable infrastructure, it would not amount to the use of force in violation of Article 2(4). Disinformation and criminal activity generally also fall below the threshold of an armed conflict. In fact, it gives an impression that 'principle of non-use of force' under Article 2(4) of the Charter has been made impotent by Grey Zone conflict.

Applicability of IHL

Classification of contemporary conflict is based on the post-World War II revision of the Geneva Conventions, which are applicable in international and internal armed conflicts. Assessing the existence of armed conflict is easy when the armed forces of states are engaged in hostilities against each other in an inter-state dispute. However, in the case of Grey Zone conflict, which

cannot be classified as ‘war or armed conflict’, the applicability of IHL remains ambiguous.

In the past few decades, high-tech advancements have altered the means and methods of warfare. Today, the means of Grey Zone conflict includes surgical operations, restrained and limited use of kinetic forces by special operations forces or irregular forces; cyber warfare; information warfare; use of autonomous weapons, and other non-violent means of coercive diplomacy such as economic sanctions, etc. The states in a Grey-Zone conflict use a mix of strategic and operational techniques, making any resolution arduous. The beginning and termination of conflict remain uncertain because most of the Grey Zone conflicts opera-tions are undertaken in highly permeable international borders. Since Grey Zone is a mix of military and non-military measures; application of IHL in the use of means and methods of conflict becomes difficult.[10]

Lawfare. Today, domestic law, international law and judicial institutions are being exploited to influence the military policies of the government. Lawfare is the strategy of using or misusing law as a substitute for traditional military means. It is becoming a powerful ‘force multiplier’, reminding one of Sun Tzu, who once said, “…. to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy’s resistance without fighting”.[11] It has become an integral element of any Grey Zone conflict. As Grey Zone conflicts become more prevalent, relevance of lawfare intensifies. It provides a means to compel specified behaviour with fewer costs than the use of weapons. Lawfare thrives on legal ambiguity and presents challenges to international peace and security by questioning the validity of existing public international law rules. For instance, PLA’s handbook on international law states that officers should not feel completely bound by international laws that are detrimental to China’s national interests but should focus on those international laws beneficial to China while evading those harmful to China’s interest.[12] Russia, China and Palestine Authority (PA) have used ‘legal warfare’ as a major component of their strategic doctrine. Lawfare is a good substitute for kinetic warfare; the states need to exploit it for strategic advantages.

Challenges for India

China and Pakistan, based on their own interests and abilities, have developed different Grey Zone strategies against India. Pakistan is relying on Grey Zone tactics using what is described as salami tactics, support to terrorism and cross border infiltrations; whereas China's actions are incrementally changing the territorial status quo. Both these adversaries are using non-military tools of coercion —such as cyber-attacks, propaganda, terrorism, insurgency and covert operations. Such activities are likely to continue using Grey Zone strategies in the coming years.

To counter a Grey Zone conflict requires a full spectrum response involving the state's security as well the private sector. Countering measures against this method of conflict will require more than traditional military strategy responses and must incorporate more than special operations forces or paramilitary operations. The members of Special Forces may have to undertake clandestine operations in the grey area between overt military operations and covert operations. These members may also have to adopt certain methods like "perfidy" which may be prohibited under IHL.[13]

Non-Lethal Weapons. Non-lethal weapons (NLWs) can also play an important role in countering Grey Zone tactics. The use of such weapons may also be strategically advantageous since conventional weapons may cause unnecessary, indiscriminate or disproportionate harm. The use of NLWs such as chemical riot agents or incapacitating agents may be an effective way of responding to unconventional Grey Zone threat that may be operating in the area dominated by civilians.

According to Fitton (2016), counter-responses to Grey Zone tactics would involve further investment in show of force, disinformation, deterrence and manoeuvring adversaries away from Grey Zone tactics.[14] Grey-Zone success depends on patience and an ability to blend together all the instruments of state power. We must remember that even a strongest enemy with well-developed armed forces and technologically advanced weapons has some vulnerability. These vulnerabilities need to be exploited at the right time and by appropriate military and non-military means.

The challenges of today are that state and non-state actors do not respect the norms and rules of the international law. Any use of force or threat to use force that is contrary to Article 2(4) of the UN Charter and that fails to meet the requirement of self-defence under Article 51 remains unlawful.[15] In order to achieve an edge in Grey Zone conflicts, India must:

- Invest in establishing and upgrading its cyber capabilities, improve the intelligence gathering effort against its potential adversaries.
- Intensify the quality and quantity of attacks on targets located near its border through limited military operations.
- The use of drone technology could be a game changer in Grey Zone conflicts and, therefore, must be exploited.
- The armed forces must invest in lawfare and devise a comprehensive strategy for its effective exploitation.
- The use of NLWs must be considered to avoid disproportionate civilian casualties in operations.

Conclusion

The ambiguous nature of Grey Zone activity, coupled with a lack of clearly defined law, makes it difficult to hold Grey Zone actors accountable and develop acceptable countermeasures. The role of non-military means of achieving political and strategic goals has grown in the last decade; they have exceeded the power of weapons in their effectiveness. Today, the internet and social media are creating entirely new opportunities for the mass manipulation of opinion. The rules of war are changing rapidly. Grey Zone conflict is a viable and cheap option when compared to a broad military operation. States engaged in Grey Zone conflicts will continue to exploit weaknesses in adversaries to increase their own relative gains. The international community must recognise that Grey Zone conflict poses a real danger to the world peace. It must ensure that Grey Zone conflict does not operate in a legal vacuum. Since IHL fails Grey Zone conflict, it needs to be updated.

Endnotes

[1] Facebook now estimates that during and after the American election in 2016 a Russian-linked troll farm called the Internet Research Agency was responsible for at least 120 fake pages and 80,000 posts that were directly received by 29m Americans. Through sharing and liking, the number multiplied to nearly 150million, about two-thirds of the potential electorate. "Waging war with disinformation," *The Economist*, (25 January 2018).

[2] Valery Gerasimov Valery, "The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, (January-February 2016), 23-29.

[3] IHL achieves this by: (i) Geneva Conventions of 1949—sparing those who do not or no longer directly participate in hostilities (for example civilians; injured, sick or wounded soldiers; or those who have surrendered or been taken prisoners of war; and (ii) Weapon ban/limiting treaties—limiting the means and methods of warfare which could be used by the adversaries. The present-day rules of IHL are contained in nearly 50 conventions or treaties dealing with matters ranging from the prohibition on the use of certain weapons which cause indiscriminate damage and cause unnecessary suffering, to those that deal with means and methods of warfare.

[4] Hoffman Frank G., "Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges," *PRISM*, 7, No. 4, (2018), 31-47.

[5] The Grey Zone, "The US Special Operations Command," (9 September 2015), 1.

[6] Morris Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, et.al, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War,* (RAND Corporation, 2019) 8-11.

[7] Elizabeth G. Troeder Elizabeth G., A Whole of Government Approach to Grey Zone Warfare, Strategic Studies Institute, (US Army War College, 2019), 38.

[8] In the future, "fake news" put together with the aid of artificial intelligence will be so realistic that even the best-resourced and most professional news organisation will not be able to make the difference between the real and the made-up news. This news can spread across social media in nanoseconds, disseminating information that would undermine the entire democratic institution.

[9] Carment David and Dani Belo, "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare," (Canadian Global Affairs Institute, October 2018), 15.

[10] For instance, in the recent past, the Chinese civilian fishing boats have caused near-collisions with US military vessels in the South China Sea, off the coast of Chinese man-made islands. The nexus between these agents and the Chinese government is difficult to prove, eluding the traditional law of state responsibility. International law or IHL cannot hold China accountable.

[11] Sun Tzu, *The Art of War* (New York: Fall River Press, 2014), 92.

[12] Kittrie Orde F., *Lawfare: Law as a Weapon of War,* (New York: Oxford University Press, 2016), 172.

[13] Article 37 of the 1977 Additional Protocol I prohibit "perfidy" and defines it as an acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.

[14] Fitton Oliver, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections,* 15(2), (2016), 109-119.

[15] Article 51 of the United Nations Charter states, "Nothing in the present Char-ter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security."

@**Wing Commander Umesh Chandra Jha (Retd)** has extensive field and academic experience in international humanitarian law, military law and human rights law. He was awarded PhD in 'Law and Governance' by Jawaharlal Nehru University, New Delhi in 2007. His work comprises 26 books and over 120 articles published in various journals and newspapers.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

Unconventional Warfare#

Major BN Sharma

Introduction

A lot of new ground has been broken in unconventional warfare by US Army. Pamphlets have been published giving characteristics of the organisation of unconventional forces, their employment and operations. It is the intention here to narrow down the generalities and apply some principles of this type of warfare to conditions obtaining on our borders, as also to suggest a possible organisation and employment of Special Forces for achieving our strategic objectives.

Historical Background

UNCONVENTIONAL forces have a very long history. Such forces were systematically employed during the American War of Independence, war on western border against the Apaches and the Red Indians, guerilla activities in the Spanish War of 1812-13, and Russians' scorched earth policy in the face of Napoleon's invasion. The Arab resistance movement led by Lawrence against the Turks assisted Allenby's operations considerably in Palestine during the First World War. The Chinese guerilla activities against Japanese invasion forces from 1937 onwards and the covert activities of communist army offer examples just prior to the World War II, while the partisan movement in Yugoslavia and the Russian partisan warfare behind Nazi forces in Russia are those from World War II. In our own country, the Marathas used these tactics with devastating effect against Aurangzeb's Mughal Army. Bush-war tactics in Algeria and communist guerilla activities in Malaya, Vietnam and Indo-China are recent examples. Communist ideological infiltration is followed by establishment of guerilla bases and then slowly the resistance movement gains momentum. At a suitable time, open hostilities break out and the power is transferred into revolutionary hands. This has been the pattern of communist revolutionary wars. All this study highlights one important lesson. That small forces highly mobile, lightly

equipped, suitably indoctrinated, operating in a friendly population, and in favourable terrain can ultimately defeat large regular forces. Their ubiquity, flexibility, power to vanish and appear at appropriate times, refusal to fight a losing action, and be fixed, are baffling to a regular army used to cumbersome, time consuming procedures and mostly road bound. Because of their devastating nature, big powers can ill-afford to use nuclear weapons. This hesitation has led to the use of cold war tactics and unconventional warfare. In fact, the future wars will mostly be bush-wars based on guerilla tactics supported by ideological infiltration. In brief, small battles and pressure tactics will be the normal pattern of all future wars.

Guerilla Techniques

In order to function efficiently against an invading army, our guerilla forces will need a friendly and sympathetic medium to work in. Whether operating deep in enemy territory, friendly neighbouring countries or in our own border areas, the guerillas should first be acceptable and then gain the confidence of the populace. For this, they should have a political ideology and emancipation programme of greater promise than the so-called communist liberation movement. This should be the natural outcome of sound political wisdom, diplomatic foresight, bold and constructive social and economic programme. The agrarian economy and feudal character of society in these regions has to be borne in minds. The political programme will have to be based on agricultural reforms, co-operative movements, productivity schemes and so on.

The religious and cultural traditions of the people should be respected and any communist attempt to falsify and misquote history should be resisted. Efficient counter propaganda machinery working with good political intentions will turn the tide of the communist suppression movement. The guerilla movement will have the normal three phases of development. First, the organisation, consolidation and preservation of regional bases situated in isolated and difficult terrain. Woven round each base should be a protective belt of sympathisers willing to supply food, recruits and information. The second phase is one of direct action. This will include acts of sabotage and terrorism against enemy

occupation forces, attack and ambush on his outposts, supply dumps and isolated garrisons. In this phase, the guerilla expansion of 'liberated areas' is carried out including political indoctrination of peripheral areas.

In the last phase, the guerilla forces seek a decision and aim at the destruction of enemy. During this phase, a large proportion of guerilla force completes its conversion into conventional force and engages enemy in conventional battles, thus, completing his destruction. Mao Tse-tung in his book has stressed upon the importance of guerilla warfare as a 'necessary strategical auxiliary' to the operations of the regular army. General Blumentritt has gone even further. He says: 'It is my belief that in a future war the fight will be directed primarily against enemy activities in rear and that battle will be sought only as an auxiliary means to achieve victory'. This is our cue. We shall do to the communist invading hordes what they did to the Japanese invasion army.

Regular Forces in Unconventional Role

There were some regular forces employed in an unconventional role during World War II. These were the following:-

(a) **Long Range Patrol Group.** These were observation elements 'deployed by the Eighth Army' for gaining intelligence about the enemy during its frequent advances and withdrawals. These were mainly patrols living out in no man's land or even enemy territory. Their task was to pass back useful information, deny some features to enemy, raid his convoys and supply dumps, and sometimes even carry special missions.

(b) **Command Forces.** These were regular forces specially organised, equipped and trained, and meant to carry out special missions. British commando raids over German occupied Norwegian Coast to destroy Heavy Water plants are well known.

(c) **Deep Penetration Forces.** Planned, organised and led by Orde Wingate, these forces operated behind Japanese lines, snapped their communications, contained some regular

enemy forces, and generally helped the operation of main forces.

Though their method of employment is novel, all forces mentioned above are still conventional forces used to assist the operations of the main regular forces.

Special Forces

What we understand by Special Forces now is forces specially organised, trained, equipped and probably dressed, employed to operate independently or in conjunction with the main regular forces under the theatre commander. Special Forces employed under the theatre commander will be trained to conduct guerilla warfare and related unconventional warfare activities. Their task will be to develop, organise, equip, train, and direct indigenous forces in the conduct of guerilla warfare. They may also have to advise, train and assist indigenous forces in counter insurgency operations. These will employ guerilla or regular tactics as required and raise resistance forces from amongst the countries where they are operating. They may be called upon to initiate guerilla movement against the established authority or resist foreign invasion by guerilla tactics, acting as partisans or to counter enemy guerilla tactics in one's own or neighbouring countries, and even in a counter insurgency operation in own country.

Characteristics

These should be highly mobile, lightly equipped, air transportable forces capable of being air-dropped and maintained. They should be kept at the highest state of readiness, ready to move to the threatened or desired area of operation at a short notice. They should be under the control of the highest strategic commander in a theatre.

The personnel of Special Forces must be volunteers suited to operate in a particular geographical terrain. They should have enough local knowledge, be acceptable to the population, and should be capable of acting as guerilla leaders for the indigenous resistance forces. Needless to say, they should be tough,

resolute, dedicated men, well versed in all skills of soldiering, weapons and tactics.

Organisation

The Special Forces group consists of a Headquarters, Headquarters Company and four Special Forces companies. Each company has an administrative detachment, one operational detachment C, three operational detachments B and twelve operational detachments A with varying tasks and capabilities. They can operate independently as guerilla detachments or in conjunction with the regular tactical field armies. Each detachment is capable of raising varying number of local insurgency battalions. The Special Forces group should be under the strategic control of the theatre commander. Each group should be capable of establishing itself alongside a theatre Headquarters and deploy its companies with army groups. Companies, in turn, deploy their detachments down to armies. Down to section level, the Special Forces should be well served with propaganda machinery in its organisation. This is vital since the main task of the Special Forces initially is to win popular opinion by offering constructive political philosophy with concrete immediate advantages to show. To counter the enemy's political indoctrination and propaganda, this machinery will have to be very ingeniously devised.

In the initial stages, Special Forces sections deployed in own, friendly or enemy territory will be busy winning public support. The second stage will be a careful study of enemy methods, tactics, and gathering all intelligence about his forces. Then the forces will start training the resistance forces for their role. Their tactics initially will be one of consolidation and surveillance; then they will expand their bases and group them into bigger bases. Still on the defensive, fighting only for capturing enemy weapons, equipment and supplies, they will consolidate their hold, indoctrinate the population or probably counter indoctrinate them. In all this, the Special Forces must understand the customs, traditions, past history of the people, their economic conditions, and political aspirations. The attitude towards the population should be one of respect, understanding, and affection. Later on when their hold grows stronger, Special Forces take to open battles and fight major actions.

All along, the Special Forces will have to be in communication with the theatre commander. Full logistical support must be ensured for the troops in addition to living off the land.

The Special Forces should be able to subsist for a long period in enemy territory, may be years, and merge with the local population in appearance, customs, habits, language, and way of living. They should have a thorough knowledge of enemy organisation, weapons and equipment, and know-how to use them.

Areas of Employment

Special Forces can operate in the following areas:-

(a) Contiguous border areas during initial invasion of own territory.

(b) Own areas lost to invaders when enemy drives through the first line of defence.

(c) In offensive operation in enemy territory ideologically and politically favourable to us.

(d) In a ring of friendly countries to contain communism and form an ideological and military barrier against enemy indoctrination military operations.

Method of Employment

Special Forces can be employed as an independent force in a friendly country to fight communist expansion. It could also be employed independently in one's own or enemy territory to wage a guerilla war. It could alternately be employed in a resistance movement to assist the operation of own main forces in offence and defence by deploying either behind the enemy or on his flanks.

Offensive Operations. In offensive operations, these forces could form the vanguard of our invasion forces operating much ahead of our advancing armies and finally having done their work, link up with the head of the advancing forces. Their work will start much earlier also. They will prepare ideological ground by starting a movement of liberation. Living with the people and indoctrinating

them, they will create out of them willing receptionists to welcome our advancing armies. They will protect the flank of the advancing army as Lawrence's Arabs at Amman protected the eastern flank of Allenby's Army. They could also indulge in a whispering campaign to discredit the enemy government by exaggerating our success and undermining his authority. Espionage, sabotage on enemy communication, mobilisation efforts and essential services, and all other fifth column tactics will be used. There are many friendly areas within enemy territory where these forces could be landed and where they can establish their bases. Our foreign refugees could form the scouts and even major portion of our Special Forces. These smuggled inside enemy territory will form the nucleus of our friendly firm bases.

Defensive Operations. In defensive operations, our Special Forces will initially be mainly employed in the harassing operations, employing typical guerilla and partisan tactics, themselves or with the help of the local population. They will be operating mainly in our own territory lost to the enemy. Our border hilly areas and neighbouring countries provide excellent terrain for such tactics. Mountains, jungles and valleys are ideal places for guerilla activities. Their main tasks will be to operate in enemy rear, harass, uproot and destroy. Hanging on enemy flanks like invisible wasps, and harassing his rear, these forces will indulge in all normal guerilla activities. Killing commanders, sniping, ambushing, holding up convoys, looting weapons and equipment, they will force on protection duties and put out of action a large portion of enemy fighting strength. Their intimate knowledge of our own territory and popular support will give them all the advantages of a partisan. Slowly as our main forces take up the offensive and prepare to counter attack, these forces will whip up their activities, gain initiative, gather momentum, enlist popular support and ultimately by employing normal tactics join up with the main forces These forces will he readily convertible from guerilla into regular troops and vice versa.

Conclusion

The time has come when we have to think in terms of our offensive response to the communist military and ideological infiltration. Placed, as we are, dangerously close to a ruthless, highly efficient, and expansionistic communist dictatorship, our democracy can ill-afford to lose sight of the handicaps of a purely defensive strategy. While closing all gaps in our own defensive set up, our eyes should seek for a chink into the enemy's armour. Well organised Special Forces, versatile, ubiquitous and well supported shall arrest further communist expansion in our own and neighbouring countries and help decisively our offensive and defensive operations.

#This article has been reproduced from the **April to June 1966 issue of the USI Journal** where it was first published.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.

Short Reviews of Recent Books

Territorial Army: Gateway for Civilians to Army. *By Lieutenant Colonel Surender Singh, (Chennai, : Notion Press; June 2020), Pages þý302, Price - Rs 400/-, ISBN-978-1648997037 (Paperback)*

The changing nature of war, and extension of war to newer sophisticated domains, has forced the administrative and military establishments across the world to relook into the role of the defence forces in protecting territorial integrity and sovereignty of the nation. The blurring line between conventional and unconventional warfare in a highly competitive and contested environment has compelled scholars to examine the concept, dynamics and organisational features of army in a newer light. Amidst heated debates over integrated commands, the book 'Territorial Army: Gateway for Civilians to Army' by Lieutenant Colonel Surender Singh is a valuable addition to the study of territorial army.

The book looks into the longue durée features of the territorial army, highlighting the role and rational for citizens' army, with very interesting anecdotes across the book, making it interesting to readers. The book runs into 300 odd pages and looks into the establishment of territorial army in India, with ample factual and contextual information. The chapter on concept of different territorial armies is short but exhaustive. The detailed nature of first three chapters makes these attractive and exciting. The chapter 3 on Dynamics of Indian Military Traditions provides ancient perspective, though the readers could have been given more details of the Great War of Mahabharata where the role of civilians is rightly emphasised by the author. The European Military roots rightly places the chapter in context of the book and, hence, gives credence to the next chapter on the role of territorials in the Great Indian Revolution of 1857. The 1857 revolution, and fear of another mutiny, prompted the raising of Volunteer Force of India. The flow of the chapter is emaculate and chronological in nature, with table and contents, making it a must read.

Territorial Forces during the World Wars is again an interesting and enriching read. However, the addition of the events post World War-I, including the dilemma over the role of territorial army within the British administration, would have added crucial

dimension to it. The complexity of relationship between British cavalry units and its political and military class after the first world war, the idea of creation of a system of decentralised administration during the reform of the territorial army in 1920s, the backlash from territorial army highlighted by other authors could have been a valuable addition.

Chapter four on post Independence organisation is again an exhaustive read with plenty of takeaways, particularly details on growth of territorial army. Finally, the author has substantially put forward his views and vision for the future of territorial army. The vision and opinion truly reflects his thorough understanding of the territorial army based on his reading, it role in the changing nature of warfare, and shortcomings, if not lacunae, in the current system. He rightly advocates the role of citizen's army in countering the emerging security challenges to the nation, which should back the regular military forces. Nowhere author has made any allusion of dismantling or reducing the true capacity of the regular forces; he, on the other hand, has recommended ways and means to support it through territorial army.

Finally, the book has painstakingly explained the various facets of the territorial army, its history and evolution, and need for it in future to counter modern security threats.

Shri Gaurav Kumar

The Coolie's Great War: Indian Labour in a Global Conflict, 1914-1921. *By Radhika Singha, (New Delhi HarperCollins India, December 2020), Hardcover Page 396, Price Rs. 699/-, ISBN-13: 9789353579852*

Until a few years ago, the number of books on the Indian participation in the Great War could perhaps be counted on the fingers of both hands; with a few left to spare. The period of the centenary commemoration of the conflict (2014-2018) saw a resurgence of interest in histories from the periphery and a number of excellent books were written on the role played by India in the First World War. These helped to create a greater understanding of the very significant impact that India had upon

the course of the war and also to examine, in turn, the outcome of the war's legacies upon India.

However, there was a piece of the puzzle that was missing. Of the approximately 1.4 million Indians who were recruited for service, nearly 5,64,000 were non-combatants or followers, the bulk of whom served in the numerous labour and porter corps' raised for service in the various theatres of the war. There was, till date, no account of the war service of this bewildering array of non-combatant followers whose numbers were used to swell the Indian manpower contribution to the war effort, by colonial authorities and Indian elites alike. This book fills that yawning gap in the story of the Indian 'contribution' and sheds light on this vital yet little known aspect of the 'war to end all wars'.

The book consists of six chapters, each touching upon different themes relating to the repurposing and deployment of Indian labour for imperial military purposes during the war. It delves into myriad aspects of this mobilisation: ranging from the geopolitical imperatives that underpinned the pre-war movement of Indian labour to the manner in which these were reframed for the purpose of attaining imperial war aims. In the process, it allows the reader to gain a better insight into not just the terms of service, and the forms of contract that governed that service, but also the manner of utilisation of Indian labour in theatres as diverse as France, Mesopotamia and India's North West Frontier. The resistance to enforced recruitment in some parts of India brought the war to the doorsteps of remote areas of the country, with repercussions on local communities that are felt till today.

This book, therefore, not only fills an important gap in the Indian military historiography of the Great War but also places the participation of these menial labourers into a larger framework of a transnational labour history. It is essential reading for all military, social and labour historians and helps to even out the overtly Eurocentric narrative of the conflict, and place it in a global perspective. Very highly recommended for all Service libraries.

Sqn Ldr Rana TS Chhina, MBE (Retd)