SYNERGY

JOURNAL OF THE
CENTRE FOR JOINT WARFARE STUDIES

CENJOWS
(Established : 2007)

Centre for Joint Warfare Studies (CENJOWS)
Kashmir House, Rajaji Marg, New Delhi 110011
Telephone Nos : 011-23792446, 23006538/9
Fax : 011-23792444
Website : www.cenjows.gov.in
E-mail : cenjows@cenjows.gov.in

Synergy is a bi-annual Journal that is published in Feb & Aug every year. It is supplied to the members of CENJOWS. Articles, Book Reviews, abridged version of Research Papers and Dissertations may be sent to the Editor as per the guidelines contained in the Journal. Advertisment enquiries concerning space and charges may also be sent to the Editor.

The Centre for Joint Warfare Studies (CENJOWS) is an independent, professional research institute established in 2007, in pursuit of strengthening the concept of 'jointness' within the defence force, as well as with other agencies that jointly contribute towards a nation's war fighting capability. SYNERGY is the CENJOWS Journal that strives to expand and deepen the understanding of issues concerning defence, national security and civil-military interface which are so very essential for joint war fighting.

Price : **Rs. 200/- INR or US 10$**

GREY ZONE WARFARE IN THE INDIAN CONTEXT

कार्पोरेशन बैंक Corporation Bank

सार्वजनिक क्षेत्र का अग्रणी बैंक A Premier Public Sector Bank

टर्म बीमा कवरेज के साथ उच्च–विशेषताओं से भरपूर वेतन खाता

Hi-Feature Salary Account with Term Insurance Coverage

कार्प पे रोल इलाइट और डिलाइट खाता

Corp PAYROLL ELITE & DELITE ACCOUNT

*Conditions apply

अधिक जानकारी के लिए कृपया शाखा प्रबंधक से संपर्क करें अथवा हमारे बैंक की वेबसाइट www.corpbank.com देखें

For more details please contact Branch Manager or Visit our Bank's website: www.corpbank.com

CONTENTS

FEBRUARY 2020

FOREWORD

Experiences of the last couple of years indicate that national political objectives are increasingly being achieved without official declaration of war. Armed forces are also employed in non traditional domains and the so-called substitute troops are beginning to play a bigger role. Wars are an extension of political means to achieve the desired end state in national interest of a nation. 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 against a powerful adversary. This process always had several built in components of grey areas such as ideological aspects, intelligence activities and psychological operations.

After the Gulf War II, the contents and colours of Grey Zone have increased manifold. Hybrid War has emerged as an effective choice and the role of non-conventional forces has come into prominence. The domain specific warfare has already graduated to a Joint Warfare concept. The new war fighting domains have led to the concept of Multi Domain Operations (MDO), where assets in one domain are employed for fighting in another domain. While MDO concepts are being fine tuned mainly in the US, the larger concept of whole of nation approach for serving the national interest have gained ground across the globe. These concepts exploit the Grey Zone and as such the term Grey Zone Warfare has gained prominence.

Grey Zone operations comprise of many components. The ideological aspect of a nation plays an important role. China's island building and subsequent control over them, widespread in the South China Sea is an example of this. Traditional Organisations would be insufficient for undertaking Grey Zone operations and hence countries would be forced to evolve organisations and structures to exploit the Grey Area. Leadership itself would require reorientation and training for undertaking these operations.

Grey Zone Warfare is waged in multiple domains and dimensions in many key battle spaces directly impacting an adversary. These domains may be widely dispersed like Maritime, Aerospace, Cyber, Intelligence Operations, Infosphere and Virtual Warfare dictated by new age technologies. Maritime domain has the greatest potential for undertaking Grey Zone operations as this global common is accessible physically to all state and non-state actors. Well known strategist-sage Sun Tzu wrote 2,500 years ago: "To win one hundred victories in one hundred battles is not the acme of skill: To subdue enemy without fighting is the acme of skill". 'Victory without fighting' hence is the end objective of Grey Zone Warfare.

Liberal democracies, constitutionally constrained by rules and democratic accountability, are at an asymmetric disadvantage and risk being outmaneuvered by states willing and able to use these tactics. India, a major world military power, has always remained in the forefront of seeking its own war fighting concepts. CENJOWS has brought out almost all components of the Grey Zone warfare in the February 2020 issue of the Synergy journal. I am sure, the articles by domain experts will assist the strategic community in understanding, exploiting and building on the emerging concept of the Grey Zone Warfare.

(R Hari Kumar)
Vice Admiral
CISC & Chairman CENJOWS

IDEOLOGICAL ASPECTS OF GREY ZONE WARFARE

Lt Gen Mukesh Sabharwal PVSM, AVSM, VSM (Retd)*

"War is fundamentally about securing strategic and political objectives. A nation that can achieve those objectives without resorting to physical force not only avoids the associated cost in blood and treasure but also may nullify its adversary's military capabilities, no matter how effective they may be".

- Timothy P McGeehan.[1]

Understanding Grey Zone Warfare

To put it simply, we associate grey with something between black and white. It usually refers to a situation that is unclear or ambiguous and wherein there is a doubt of its place within two extremes. The term "grey zone warfare" has come to surface in the last decade, especially in Western security related literature, with the Americans using 'grey' and the British community referring to it as 'grey' zone warfare or the space generally between war and peace. As expected, both proponents and opponents differ with the definition or understanding of the term and the debate continues. Scholars, practitioners, and security experts alike have been finding it difficult to come to terms with fixing labels such as "hybrid wars", "asymmetric", "fourth/fifth generation wars", and "grey-zone" conflicts to distinguish contemporary scenarios from those of conventional or traditional wars.

The grey zone involves coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events. The grey zone concept has been propagated by experts and analysts in the United States to

distinguish it from the 'Global War on Terror' being fought by them over the last two decades, ever since the closure of the Cold War. The Russian doctrine has often been termed as 'hybrid war' by the Western world. As a response, President Putin's press secretary, Dmitri Peskov remarked in 2017, "If you call what's going on now a hybrid war, let it be hybrid war. It doesn't matter: It's war".[2] Fourth generation war, on the other hand, suggests external intervention in the internal affairs of a target country. It essentially employs subversive means, such as undermining peace and stability; inspiring isolated terrorist incidents; communal and religious divisions; and trying to destabilize the economy by pushing in counterfeit currency.

A leading expert, Echevarria Antulio[3] is of the view that grey-zone wars are distinct as they sit below NATO's Article 5 threshold, and below the level of violence necessary to prompt a UN Security Council Resolution. He provides illustrations like the aggressive moves undertaken in recent years by Moscow in Ukraine and by Beijing in the South China Sea. In each of these cases, there was little or no legal premise for a military response by the West; hence, the tendency to refer to such hostile actions as grey-zone wars, that is, use of military force that fall short of actual war but which definitely do not qualify as peace.

The grey zone concept is more similar to political warfare than to hybrid warfare. Part of its understanding is that the means adopted to pursue the ends are of great political significance, similar to those that could only be achieved through warlike aims.[4] In any case, the grey zone can be an alternative to hybrid warfare and since they are compatible, one single strategy can include both options, which will also provide greater flexibility.

Conceptual Approach of the United States

Several US security professionals expect the competition to be played out primarily below the threshold of major war—in the spectrum known as the *grey zone*. The 2017 U.S. National Security Strategy and the publicly released summary of the 2018 National Defense Strategy agree on one fundamental theme: The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia

and China. In the National Security Strategy, the White House argues that "China and Russia challenge American power, influence and interests, attempting to erode American security and prosperity."[5] In the public summary of the National Defense Strategy, the Defense Department argues that "Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security," and it suggests that: the central challenge to U.S. prosperity and security is the re-emergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.[6]

The U.S. Chairman of the Joint Chiefs of Staff, Gen. Joseph Dunford, suggested in 2016 that Russia, China, and Iran employ "economic coercion, political influence, unconventional warfare, information operations and cyber operations to advance their interests and they do it in a way that they know we don't have an effective response. They, unlike us, are able to integrate the full range of capabilities their states possess to advance their interests." The traditional U.S. mindset in which "we are either at peace or at war is insufficient to deal with that dynamic," because the emerging situation is primarily "an adversarial competition with a military dimension short of armed conflict."[7] Grey Zone conflicts or shadow wars are not a formal type war. They are not traditional conflicts or full scale wars between nations or states. The recent examples are the Russian shadow war in the Crimea, the growth of ISIL in the Levant, and the Boko-Harim incursion into West Africa.[8]

The United States philosophy being expeditionary in nature, it follows an approach entailing special forces conducting foreign assistance training and advisory operations to the indigenous forces of the conflict. The main effort for the approach is to build partnership capacity of indigenous force that can provide security and stability of the human domain of the Grey Zone. Special forces are an economy of force that can provide a surgical strike capability, to protect the indigenous populace from both internal and external enemy threats. The surgical strike effort or direct approach can offset the enemy, until sufficient indigenous forces are available to deny an adversary a

decisive advantage on the Grey Zone populace. A small foot print on the ground of special forces teams working with indigenous proxies in Grey Zone is a viable option to respond and deter shadow wars. In Grey Zone conflicts, defeat of the enemy may not be attainable nor is the word "defeat" applicable to the conflict. Special Forces must think in terms of negate, controvert or dis affirm the enemy from the human terrain. "Operational art is the thoughtful sequencing of tactical actions to defeat a component of the armed forces of the enemy"[9]

Perceived Russian and Chinese Concept

Grey zone strategies generally combine a number of tools such as political, diplomatic, informational, covert or cyber in a way that are intended to achieve strategic ends over time without triggering a conventional and high risk armed conflict. Not all grey zone strategies are gradual though. For example, the Russians set conditions to rapidly seize Crimea using little green men, criminal organizations, and disaffected locals. Once this feat was completed, the West faced a dilemma: do they risk war to liberate Crimea from Russia; let Russia keep it; or execute their own grey zone strategy to impose costs on Russia for their transgression of international norms?

Although Russia has long employed information as a tool of state power, since 2013 its military thinkers have increasingly adopted a novel approach of keeping information at the forefront of their strategy. The logic of information operations often guides Russia's coordinated military, diplomatic and economic efforts. Scholars and policy makers have used many phrases, such as new generation warfare, hybrid warfare, new-type warfare and non-linear warfare, to describe their contemporary military doctrine.[10]

The Russian Ministry of Defence defined information warfare as the ability "to undermine political, economic and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interests of the opponents".[11] Russia's information operations maintain continuous activity as the nation is always in a declared or undeclared war.[12] A hybrid force of state and coerced or co-opted non-state actors execute information confrontation. This force

promotes the state's carefully crafted emotional appeals to manipulate a variety of audiences.[13] Russian diaspora populations exist throughout its neighbouring countries, Western Europe and the United States. Russia's foreign policy seeks to influence all Russian compatriots, including citizens living abroad, immigrants from former Soviet Union and descendants of compatriots.[14]

China uses a grey zone approach in the South China Sea that not only uses a wide range of tools short of war, they also employ their conventional forces as a not so veiled threat to anyone that challenges the illegal behavior of their paramilitary fishing fleets and other activities. Their actions seem to fall well short of established triggers for military action by either the United States or the target of the grey zone coercion. The goal is to avoid major clashes, unambiguous or attributable violations of international law or norms, or outright conflict.[15] This characteristic guides their choice of specific actions, such as cyber harassment or creating a de facto presence in a maritime area, especially the South China Sea and it can also help shape the character of a grey zone campaign over time. In addition to the disinformation and propaganda techniques, China is known to apply in its strategy the elements of legal, media and psychological warfare.

Ideological Features of Grey Zone Warfare

Grey zone campaigns are first and foremost non-military in structure. The basic elements used are diplomacy, political, information and cyber warfare. The kinetic element employed is usually militias or non-state actors. The objective is to operate with such means that do not give any impression of it being military in nature. This is also done with a purpose to elicit a non-military response.

Another feature of grey zone warfare is an ease of deniability. Actions by the aggressor are more often than not undertaken by proxy players or non-state actors. The aim of this is obviously to show to the world that they are not responsible and nothing should be pinned to their collar. Disinformation campaigns and the use of cyber attacks are the order of the day as it is difficult to attribute them to the originator.

A significant characteristic of grey zone warfare is that its intensity is carefully controlled in order to keep it below the threshold of regular or conventional war. The basic purpose is to avoid threatening the opponent's vital interests so as not to elicit a response. The provocation is thoughtfully calibrated for it to significantly instigate, yet not cross the limit of acceptability and tolerance. The targets are therefore selected very deliberately from a point of view of proximity, accessibility and a lower likelihood of reaction. The risk of escalation is also meticulously factored in during the planning stage, including more aggressive kinetic action if the need arises.

Grey zone conflicts focus on the weaknesses of countries being addressed. Vulnerabilities such as status of ethnic population aligned to the aggresor or religious polarisation or weak economic condition and internal disparities are potential targets. Participation of locals, disillusioned elements and even the diaspora are exploited.

As the grey zone environment is non-military in nature, the country's defence ministry nor their military is at the forefront of such a campaign. These are more of a whole of government approach with the application of all relevant instruments of power. Political, diplomatic, informational and cyber domains are characteristically in the lead.

Warfare of the grey zone variety is the preferred choice of authoritarian and totalitarian states where no questions are asked of the perpetrators and no explanations are offered. It is difficult for liberal democracies to emulate such kinds of warfare due to constitutional constraints, responsibility to citizens and accountability to elected institutional bodies. Their response is expectedly reactive, controlled and delayed.

Technology is an essential feature for grey zone operators. Developments in the ICT domain provide further acceleration to ingenious information warfare campaigns. More sinister designs are expected in the future with the advent of IOT, AI and Blockchain types of technologies.

Indian Context

India has been involved in several conventional wars since its Independence in 1947 with its neighbours Pakistan and China. The

geo-political structure of South Asia emphasizes its Indo-centricity. India is several times larger in population and size than any other country in South Asia. Its predominance not only in geographic characteristics but its economic prowess makes its neighbours apprehensive. India's security relationship with its neighbouring countries therefore, is often characterized by a lack of trust. In the seven decades since Independence, its internal security situation has undergone a change. It is affected not only by several insurgencies in North East and Central India, but is equally if not more, impacted by terrorism sponsored, guided and supported from across its borders in Jammu and Kashmir (J&K).

A close analysis of the features of grey zone warfare, to determine its applicability in the Indian context, indicates a fair degree of similarity. Although the grey zone concept is relatively recent, its characteristics appear to have been followed by China and Pakistan in similar measure albeit using different terminologies.

Pakistan has been waging a proxy war in Jammu and Kashmir since 1989. Its aims in this regard are apparently to continue to wage a low-cost war against India, using terrorists rather than military forces; to bleed the Indian Army through attrition; to project insurgency as home-grown but finding it difficult to sustain the terrorism in the hinterland without infusing leadership from across the Line of Control. Pakistan continues to deny its involvement, while it continues to fan the flames of terrorism in J&K, besides spreading fundamentalism in the rest of India as well.

The proxy war sponsored by Pakistan has now been going on for over three decades without any likelihood of resolution. Such a dynamic of protracted limited conflict is created when both rivals prefer to maintain low intensity violence rather than escalating to an all-out war. This situation prevents the militarily stronger side from exploiting its superiority thus leaving the weaker side with a sufficient response, even though the capability to escalate their actions exists. The superior rival fears escalation because it analyzes the cost as outweighing the possible benefits. The fear of over- escalation stabilizes the situation. However, reality shows that weaker parties are willing to take risks based on the assumption that the stronger opponent is unwilling to escalate. A dynamic evolves with the acceptance of a level which both sides can

live with. A similar example is that of Israel and Hamas failing to achieve their goals against each other. Israel has many means, superior military strength, impressive economic capability and significant international support. Hamas has invested considerable fortune and time to build a varied terrorist and guerrilla capability. Their failures are not due to bad strategy but to the natural dynamic of such conflicts. Changing the strategic situation will be possible only as the consequence of a significant politico-diplomatic move or war.

As far as China is concerned, there are three areas where grey zone activities have been evident. First, the intrusion activities along the Sino-Indian LAC; second, the China Pakistan Economic Corridor (CPEC); and third, attempt at domination in the Indian Ocean. Over the years, China's undesirable activity along the LAC and intruding into Indian territory at Sumdo, Chumar and so on, allegedly claimed by it, is a matter of serious concern but Chinese border troops cleverly keep it below the threshold of conflict. Their road building at Doklam in Western Bhutan is a classic case of intimidation and raising tension in a sensitive area through a neighbouring country. Such activities are unlikely to lead to military confrontation but definitely affect peace and tranquility in the region. The CPEC affords strategic advantage to both China and Pakistan while it effectively balances India. As the corridor passes through POK, any reaction by India will directly impact Chinese assets and interests. Presence of PLA troops in POK further exacerbates the tenuous situation. India does not endorse the CPEC but currently all she has done is to lodge formal protests. Access to the deep-sea port of Gwadar will also facilitate the PLA Navy to establish its presence in the Indian Ocean. This will enable it to protect her maritime trade from the Middle East and investments in Africa.

Conclusion

Grey zone warfare appears to be relatively recent as its terminology makes us believe. However, if one reflects on earlier conflicts and campaigns, many similarities come to the fore. Western country terminologies relating to conflicts below the threshold of conventional war reflect a certain bias. The experience of the US is primarily one of intervention in the Third World. This is also true of several colonial powers involved in bitter conflicts in their erstwhile colonies. Such operations

are expeditionary in nature. There has been a change after the end of the cold war, especially in the 21st century. With the emergence of China and Russia to challenge the US in a multi-polar world, a non-military approach has taken centre stage. While deterrence philosophy is still prevalent, the political, informational and cyber domains have assumed greater importance. By employing information operations as a decisive tool of state power, a country can press its offensive advantages in the information domain to nullify its relative weakness in other domains.

As the spectre of large-scale conventional or regular war diminishes, nations are likely to exploit the grey zone space to achieve their political objectives. They would bank upon the indecisiveness and perpetual delays in response by the target countries due to the compulsions caused by their democratic systems of governance. Meticulous planning based on well-appreciated contingencies and quicker response mechanisms along the escalatory ladder will perhaps be required on behalf of the targeted state.

***Lt Gen Mukesh Sabharwal, PVSM, AVSM, VSM (Retd)** is former AG and GOC 15 Crops & a Distinguised Fellow of CENJOWS, New Delhi

References:

1. Timothy P. McGeehan: “Countering Russian Disinformation”, Parameters, Vol. 48 No 1, Spring 2018, and p50.
2. Dmitri Peskov, quoted in Jim Rutenberg, “RT, Sputnik and Russia’s New Theory of War”, New York Times Magazine, September 13, 2017.
3. Echevarria J. Antulio II, “How Should We Think about “Grey-Zone” Wars?” *Infinity Journal*, Volume 5, Issue 1, Fall 2015, pp16-20.
4. *Josep Baqués,* “Towards a definition of the ‘grey zone’ concept”, Research Document 02/2017 of the Spanish Institute for Strategic Studies (IEEE)
5. White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017, pp. 1–2.
6. U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military’s Competitive Edge*, Washington, D.C., 2018, pp. 1–2.

7. Colin Clark, "CJCS Dunford Calls for Strategic Shifts; 'At Peace or at War Is Insufficient,'" *Breaking Defense*, September 21, 2016.

8. Dave Betz, https://smallwarsjournal.com/jrnl/art/grey-zone-conflicts-may-be-the-new-normal-but-will-have-the-same-marginal-success

9. Kelly, J., & Brennan M. (September 2009). Alien: How Operational Art Devoured Strategy. *Strategic Studies Institute Journal*, Strategic Studies Institute, U.S. Army War College. Carlisle, PA. ISBN 1-58487-402-3, Page.98.

10. Timothy. L. Thomas, "The Evolving Nature of Russia's Way of War," Military Review 97, No 4 (July/August 2017).

11. Conceptual views regarding the activities of the Armed Forces of the Russian Federation in Information Space (Moscow: Russian Ministry of Defence, 2011) quoted in Timothy L Thomas, "Russia's 21st Century Information War", Defence Strategic Communications 1, No 1 (Winter 2015): 12.

12. John Chambers, "Countering Grey Zone Hybrid Threats: An Analysis of Russia's New Generation Warfare" (West Point, NY: Modern War Institute, 2016), 26.

13. Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Before the Senate Intelligence Committee 115th Cong, (March 30, 2017).

14. Heather A. Conley, "Russian Soft Power in the 21st Century (Washington, DC: Center for Strategic and International Studies, 2011), 12.

15. Amy Chang, Ben FitzGerald, and Van Jackson, *Shades of Grey: Technology, Strategic Competition, and Stability in Maritime Asia*, Washing- ton, D.C.: Center for a New American Security, March 2015

ORGANISATIONAL REFORMS FOR THE GREY ZONE CONCEPT IN THE INDIAN CONTEXT

Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd)*

"The categories of warfare are blurring and no longer fit into neat, tidy boxes. One can expect to see more tools and tactics of destruction from the simple and sophisticated means being employed simultaneously in hybrid and more complex forms of warfare."

Robert M. Gates, US Secretary of Defence

Preamble

The current turbulent and dynamic geo-political, economic and security situation in an emerging multi-polar world, warrants all Nations to carry out dynamic strategic balancing and live in an era of 'persistent engagement' of cooperation, competition, confrontation and even conflict if national interests, sovereignty and integrity are threatened. Niche game changing technological advancements, globalization under threat, internet of things and emergence of multi-domains (MD) for intervention, to include space, cyber, electromagnetic spectrum (EMS), psychological (PSYOPS), information influence operations (IIO) available to nations, groups and even individuals at a cost, has blurred and overlapped the distinction between war and peace, spectrum of conflict, space, time, geography and even levels of conflict. Carrying the truism of 'Wars are fought by Nations not militaries' further in today's security environment, we can say that competition, confrontation and naturally conflict are a nations responsibility and obligation. India an emerging regional power with matching requirement of strategic space, resources, trade and allies aspires (and expected by allies and Asian nations) to be a Net regional security provider in the IOR and region.

In this new era of power competition, our nation's adversaries seek to achieve their strategic aims, short of conflict, by the use of layered stand-off in the political, military and economic realms. Should conflict come, they will employ multiple layers of stand-off in all domains--land, sea, air, space, information, EMS and cyberspace--to diffuse our comprehensive national power (CNP) in time, space, and function in order to defeat us. The answer lies in rapid and continuous integration of all domains of warfare to deter and prevail as we compete short of armed conflict. If deterrence fails, the armed forces as part of national multi-domain, integrated theatre operations must create a security environment during competition and confrontation stage resulting in freedom of manoeuvre to defeat/neutralise enemy systems, formations and objectives and to achieve our own strategic objectives; and consolidate gains to force a return to competition on terms more favorable to us. China along with its collusive partner Pakistan (and other South Asian allies if possible) would like to expand the battlefield, indulge in 'Grey Zone Operations' in time (blurred distinction between peace and war), in domains, and geography (overlapping of levels from strategic to tactical, no flanks or front and rear) to paralyse India and achieve their political aim (ultimately wars are fought for political and economic reasons) without actual kinetic action. We must expand our strategic aim of credible deterrence and punitive deterrence against China and Pakistan respectively, into the Grey Zone, as that's how wars (confrontation and conflict) will be fought.

Grey Zone/Multi-Domain Warfare

"War's not black and white; it's grey. If you don't fight in the grey area, you're going to lose"

Marcus Luttrell

"Grey Zone" refers to a space between the peace-conflict continuum, the methods for engaging our adversaries in that environment have much in common with the political warfare that was predominant during the Cold War years. George Kennan, described it as "the employment of all the means at a nation's command, short of war, to achieve its national objectives," including overt measures such as white propaganda, political alliances, and economic programs, to "such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological

warfare, and even encouragement of underground resistance in hostile states"[1]. Numerous names are being propounded for confrontation and conflict short of actual war. Grey zone includes nuances of MD/ Hybrid/4&5G/sub-conventional/unrestricted/non-kinetic and cognitive operations. In my opinion, multi domain is the larger picture of operating and using multiple domains both kinetic and non-kinetic/cognitive in war and peace 24X7, while the Grey Zone are the activities prosecuted between peace and war mainly in domains of diplomacy, politics, economy, social movements, communications, cyber, information, psychological, the grey spaces of insurgency and proxy war to dominate or counter adversaries conducting similar activities. Intrinsically, they are all forms of activities between Nations short of actual armed conflict. It is this concept one is referring to when writing about Grey Zone/MDO. Non-kinetic operations like information influence operations and PSYOPS also cause physical casualties like IS running over Northern Iraq in 2014 and lynching's in our heartland based on fake news/rumours. In this borderless battlefield, it is no longer possible to rely on mil forces and weapons alone to achieve national security in the larger sense[2]. Grey Zone conflict conduct is not with blunt mil power, but an all domain approach and strategic shaping of the battle space. In conventional wars, non-military targets are avoided as a matter of principle, but hybrid/ grey Z has the advantage that an adversary is able to engage both mil and non-mil targets simultaneously. The erosion of state, polity, and society is achieved at a rapid pace. Consequently, India needs domain specific and cross-domain offensive and defensive plans worked out for contingencies/nations (specially collusive China and Pakistan, and their opportunistic allies). Our 'Land Warfare Doctrine-Indian Army 2018[3]' talks of non-contact and hybrid domains of conflict which are being integrated into the conventional and sub conventional realms and could be non-declaratory and non-attributable in its execution; a characteristic of Grey Zone Warfare that needs to be catered for. An important mandate is of enhancing capabilities to address the challenges of cognitive domains

1 George F. Kennan, "Policy Planning Staff Memorandum," May 4, 1948, National Archives, RG 273, Records of the National Security Council, NSC 10/2, available at <http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm>.

2 Major John A Van Messel, 'Unrestricted Warfare: A Chinese Doctrine for Future Warfare?' accessed online on 02 Jan 2020.

3 Land Warfare Doctrine-Indian Army 2018 accessed on the net on 08 Jan 20.

of conflict viz cyber, space and information as a component of our National strategy for non-contact warfare to cause unaffordable losses to potential adversaries. An important aspect of Grey Zone/MDO is that the environment being operational, it is also grounded in physical spaces. Abstract aspects more evident in some domains are also grounded physically, despite their predominantly immaterial presentations. At some point, all the abstract elements (cognitive, virtual, informational, and human) demonstrate their effects physically at a place or in an area through a system or people[4].

Thoughts on Structures and Organisations by Major Powers

The major powers have conclusively recognised and deciphered that to maintain and expand strategic space, they need to prosecute 24X7 MDO in an era of 'persistent engagement', and the 'Grey Zone' needs to be dominated, especially against players whose geo-strategic-political-economic-military status dictates operating in the grey zone for their own (authoritarian leaders, or illiberal groups to include terrorist organisations, and even MNCs and powerful individuals) gains. Today, it's a matter of perception as to who is liberal, democratic and operates within the world order making the security situation unstable and increasing the probability of confrontation and conflict. Ironically, it is the interplay of relationships between the major powers USA, Russia and China which has acted as a trigger to promote 'Grey Zone/MDO 24X7. Russia, China, Iran, Pakistan, North Korea as numerous others have demonstrated a finely tuned risk calculus. Russia belligerently works to expand its sphere of influence and control into former Soviet or Warsaw Pact territory to the greatest degree possible without triggering a NATO Article 5 response. China knows that its assertive actions aimed at expanding its sovereignty in the South and East China Sea fall short of eliciting a belligerent US or allied response. Iran has displayed an

4 Paraphrasing from 'The Road to Multi-Domain Battle: An Origin Story' by Kelly McCoy| 27 Oct 17. Origins of Multi-Domain Battle can be traced back to 08 Apr 15 at the US Army War College, where then Deputy Secretary of Defense Bob Work charged the US Army to get after Air Land Battle 2.0. "Multi-Domain Battle" made its first appearance in Army doctrine with the release this month of the updated Field Manual 3-0; Operations and as a draft operational concept, documents that provide insight into how the army sees itself fighting tonight, tomorrow, and in the future.

impressive degree of sophistication in its ability to employ an array of proxies against US and Western interests. The epitome of isolationism North Korea is playing the rogue nuclear trigger card to the hilt to extract maximum concessions and strategic space. Pakistan with the backing of its collusive global partner China is waging a state sponsored proxy war against India. Political and grey zone warfare is played out in that space between diplomacy and open warfare, where traditional statecraft is inadequate or ineffective and large-scale conventional military options are not suitable or are deemed inappropriate for a variety of reasons.

China[5]

PLA approach to modern warfare to include training, organisation and equipping for over the past two decades has been thoroughly influenced by systems thinking. It sees modern military conflict as a confrontation between opposing systems, or what are specifically referred to as opposing operating systems. War has changed drastically from the traditional wars to a contest among numerous adversarial operating systems and referred to as systems confrontation. A Nation needs to dominate at least in part all above systems, as it is not possible even for global powers to dominate all domains at all times. Chinese most recent White Paper states that the PLA'S "integrated combat forces …. [are to be] employed to prevail in sys-vs-sys operations featuring dominance, precision strikes, and joint operations."[6] The Chinese go onto identifying four objectives to paralyse enemy's operating systems. First, degrade or disrupt the flow of information within the adversary's operating systems. Second, degrading or disrupting that operating systems essential factors, which include, but are not limited to, its command and control, reconnaissance, intelligence and firepower capabilities. Third, degrading or disrupting the operational architecture of adversary's op systems which include physical nodes. Finally disrupt the time sequence and/or tempo of the enemy's operational architecture. This is to degrade and ultimately undermine the operating systems own "recce-control-attack-

5 Referred to numerous articles and magazines to include 'Systems Confrontation and Systems Destruction Warfare: How the Chinese PLA need to wage Modern Warfare', by Jeffrey Ehgstom; www.rand.org publication; accessed on 28 Dec 2019.

6 China's Military Strategy, Beijing: The State Council Information Office of the People's Republic of China, 2015,

evaluation-process."[7] The Chinese identified undermentioned main operating systems which are Command and Control (specific service as also integrated systems); Command Info, Intelligence Information Transmission, Firepower Warfare Strike, Recce Intelligence System, Support Systems and Field Area Comunication operating systems. Modernisation, re-structuring and reorganising of PLA under President Xi Xinjian is a main priority ensuring strategic and operational integration and synergy, capacity and capability building of PLA to compete as a super power with USA (initially in Asia using A2AD capability and building capability to carry the fight to his heartland). Integrated five theatre commands, blue water Navy, strategic support force, rocket force, potent Special Forces, Rapid Action formations, Brigadisation, realistic ground exercises, strategic lift are some of the major steps taken. The Chinese are responsible for USA to re-evaluate its concepts and force structuring by creating A2AD capabilities and has always propagated 'unrestricted warfare' since centuries.

Russia

Russia's exploitation of the grey zone is not new, the prevalence of these tactics is more significant today than any time since the end of the Cold War. Disinformation, political influence, and economic and energy coercion are the core of the Gerasimov Doctrine's emphasis on the non-military means to achieve security goals[8]. The European Commission recently released a report which found that Russia undertook a "continued and sustained" disinformation campaign that targeted Europe's May 2019 parliamentary elections. Russia is also using intrusive diplomacy, influence buying, and economic threats to bring international conditions in line with its interests. Presenting perhaps the greatest risk for military escalation beyond the grey zone is Russian use of disguised forces. In Ukraine, Syria, and the Central African Republic, for instance, Russia has deployed a paramilitary mercenary organization, the Wagner Group. Last year, U.S. military forces successfully struck Wagner Group positions in Syria. The Russians may be the most audacious grey zone actor, but

7 Li Yousheng, Li Yin and Wang Yonghua, eds., Lectures on the Science of Jount Campaigns, Beijing: Military Science Press, 2012, p.74.

8 Russia in the Grey Zone, Centre for Strategic and International Studies (CSIR) by Kathleen Hicks, July 25, 2019, accessed on 31 Dec 19

they have plenty of company in the space. China, North Korea, and Iran are also engaged in many of the tactics described above. This includes improving its intelligence warning to capture a broader set of indicators and better recognize rivals' campaigns from ambiguous patterns. Above actions illustrate that Russia has managed to synchronise both the strategic to tactical security actions, as also multi domain synergy when it comes to national interests, and is also undergoing rapid structural and organization changes. Undeniably, grey zone operations has allowed Russia to punch much above its current weight and be a big player in Middle East, Africa and other parts of the world.

USA - Preparing for Grey Zone/MD Structures and Organisations[9]

The very concept of MDO and Grey Zone warfighting was conceptualized by USA. Highlighting their baby steps for structural and organizational changes, they have created and are exercising MD formations in grey zone operations. The Army has begun a rigorous process of experimentation and analysis to further inform and refine the U.S. Army in MDO concept. In 2017, the Chief of Staff of the Army directed the design and testing of Multi-Domain Task Forces (MDTFs) as forward-stationed formations able to execute aspects of MDO. Designed to deliver long-range precision joint strike as well as integrate air and missile defense, electronic warfare, space, cyber, and information operations, the MDTF operates across all domains, the EMS, and the information environment in both competition and conflict to provide the Joint Force and coalition with new capabilities to enable the defeat the adversaries' anti-access and area denial strategies. Given its capability to compete and provide and initial penetration, the MDTF, as a forerunner to other multi-domain formations now in development, is the essential first step to realizing an MDO-capable Army by 2028. The experimental MDTF under the US Army Pacific has executed a multi-year joint and

9 Accessed numerous TRADOC documents and articles (Think Tanks, Magazines and even articles on mainstream print and online media) on Multi-Domain Warfare/Environment/Operations to include 'The US Army in Multi-Domain Operations 2028'; Tradoc Pamphlet 525-3-1; www.tradoc.army.mil; Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040, Version 1.0 December 2017; Modern War Institute at West Point; www.mwi.usma.edu; Putting the Enemy between A Rock And A Hard Place: Multi-Domain Operations In Practice by Curt Taylor and Larry Kay; 27 Aug 19

combined experimentation program to inform future MDTF design. This experiment combined 17th Field Artillery Brigade with an augmented headquarters element, a joint intelligence, cyberspace, electronic warfare, and space (ICEWS) component, and other tasked organized formations to provide realistic assessments of concepts and capabilities and gather warfighter feedback to inform both Army plans and concept development. They envisage that during conflict, MDTFs will prosecute successful combat operations through early attrition of the adversary's anti-access and area denial systems and supporting combat forces from the inside, thereby re-enabling joint and combined maneuver held at risk today. Over numerous experiments and exercises in 2018, the MDTF successfully linked systems and Services across all domains, the EMS, and the information environment in ways never previously accomplished. Joint and combined components demonstrated new ways to share surveillance and targeting capabilities in support of combined schemes of manoeuvre. Most significantly, the MDTF demonstrated methods of employing layered non-kinetic effects (EW, space, cyberspace, and information operations) that helped set the conditions for successful combined kinetic engagements against both maritime and airborne targets. US Army Pacific's efforts have provided critical lessons for both the Army and the Joint Force and are enabling faster, and effective transitions of MDO from concept to fielded capabilities. Joint Warfighter Assessment (JWA) is the Army's capstone multi-echelon live and constructive exercise intended to demonstrate and assess future force concepts and capabilities required for a more lethal, expeditionary, and agile force. The US Air Force, Navy and Marines while initially reluctantly are whole heartedly participating to arrive at suitable organisations for MDO. This is being overseen at the highest political and military levels.

Organisational Reforms for Grey Zone/MDO

It is very important to note that organizational structures and reforms both at the strategic realm and military are a work in progress and mainly aspirational even amongst the pioneer powers. All of them are working with the certainty that future security and conflict environment will be multi-domain, multi-polar and 24x7. Another interesting deduction is that grey zone/MDO during peace, competition and major component of confrontation stage is planned and tasked at the national and strategic level. The Armed Forces continue to mainly focus on war fighting (including the present extra focus on Grey Zone/counter terrorism

operations) and attrition activities, with increasing capability and capacity to prosecute offensive and defensive non-kinetic Grey Zone/MDO at all levels down to tactical. Therefore, the organisational and structural reforms envisaged, need to be rooted in the current structures, cause least turbulence, and be phased depending entirely on our increasing synergy, jointness, capabilities and capacities. Change for the sake of change and peer pressure needs to be avoided as our threat scenario, technological threshold, HR management, economics, geo-political landscape and geography are very different. One is very happy to note that the same is happening in India due to strategic and operational compulsions, due to our rather dynamic regional security environment. In our context, planning, decision making and broad tasking will be at the PMO, CCS, Ministerial and NSA level with suitable support from the DPC, CDS and Service HQ level. Executive actions required of the Armed Forces will be implemented as directed by the PCOSC (Permanent Chiefs of Staff Committee). Each system and interlink will be unique and mission specific; and only some or all the systems may be created depending on the adversary and mission. Naturally the systems need to be 'seamlessly linked'. The systems and organisations of great powers specially China need to be analysed in detail. India must look towards a campaign mindset (numerous plausible threat contingencies from peace to war and MD) to proactively shape conditions in its favour, building from its strengths, not primarily from its fear, and respond effectively when vulnerabilities are exploited. This naturally requires improvements in our government policies, authorities, and capabilities, and structures and organisations at the National level. They exist but need a road map, focus and synergy.

Policy Making regarding Security Architecture in India[10]

It is pertinent to carry out an overview of security policy making in India. The Government of India with its civil services machinery has a

10 Notes from numerous papers and publications to include 'Policy Making in India: Who's behind it?' By Archit Puri dated 26 Aug 2017 in Indian National Interest; www.nationalinterest.in accessed on 07 Jan 20; RSIS Monograph No. 27, 'National Security Decision-Making In India' by Bibhu Prasad Routray; S. Rajaratnam School of International Studies, https://www.files.ethz.ch/isn/163172/monograph27.pdf accessed on 10 Jan 20. 'National Security Decision Making: Overhaul Needed' by Gurmeet Kanwal, 26 Aug 14, IDSA Comments; 'National Security Decision-Making Structures for Europe', RAND Europe, www.rand.org accessed on 05 Jan 20.

monopoly over policy decision making and implementation in the country. Overall, government policy making institutions often tend to become risk-averse. They are plagued with bureaucratic inefficiencies and lack of specialisation. Think Tanks are a good mode/option to tap, and Indian government is already reaching out to think tanks due to their nuanced research capabilities (quality of research and institutional attitude differs from shallow to highly professional). Funding is also becoming less of an issue with think tanks tapping into Indian corporates and foreign donors. Some vital policy making offices/institutions are listed below.

- **Prime Minister's Office (PMO)**: Institutions under the PMO have a wide range of responsibilities. Directly controlled institutions include the National Security Council (NSC) which has the National Security Council Secretariat (NSCS), Strategic Policy Group (SPG) and National Security Advisory Board (NSAB), and the Research and Analysis Wing (RAW) which is responsible for international intelligence collection. The PMO administratively controls the National Technical Research Organisation (NTRO), which is directly responsible for the National Institute of Cryptology Research and Development as well as the National Critical Information Infrastructure Protection Centre.

- **The Cabinet Committee on Security (CCS)**

- **Ministry of Finance (MoF)**: The Central Economic Intelligence Bureau (CEIB) operates under MoF. It directly controls various intelligence agencies that deal with economic offences.

- **Space.** Government of India, recently put out a draft Space Activities Bill to essentially regulate the space activities in India. The Act has not specified any specific Department or body within the Government of India to take ownership of regulating space activities. Today, space activities require multiple inter-ministerial as well as inter-departmental inputs today. It is a vital part of our security architecture.

- **Information, Media, Cyber Policies and Regulations.**

Decision-making power in the Indian media regulation is fairly centralized, with the central Government and ministries making the final calls when it comes to new policies and appointments. Politicians have a keen interest in news media regulation owing to the high degree of political ownership

in the sector. Thus, political and electoral logic shapes media regulation. The New Media Wing (NMW) and the Electronic Media Monitoring Centre (EMMC) come under the Ministry of Information and Broadcasting (MIB) and are involved in media surveillance along with the Ministry of Home Affairs (MHA). The National Intelligence Grid (NATGRID) which keeps all sorts of citizen data in a single database that can be accessed by officers from RAW, CBI, IB etc., comes under the MHA. The National Cyber Coordination Center (NCCC) and the National Crime Records Bureau (NCRB) also come under this ministry. The Ministry of Communication and Information Technology controls CERT-In, the Indian Computer Emergency Response Team that performs emergency cybersecurity functions and releases annual reports of security incidents. The proposed National Media Analytics Centre (NMAC) and Digital Swachhata Kendra (DSK) will also come under the MCIT. NMAC will monitor and analyse content on the internet and counter negative content, while DSK will look to deal with malware and botnets. The Department of Electronics and Information Technology (DEITY) operating under the MCIT is responsible for ensuring cyberspace security, other than delivering government services online and promoting the IT sector. Given its strategic importance the Govt has ordered establishment of the 'Defence Cyber Agency'[11].

- **Institutes which focus on external security**. Apart from R & AW, the Defence Intelligence Agency (DIA) operates under direct control of Ministry of Defence (MOD). Global Cyber Issues Cell operates under the direct control of the Ministry of External Affairs (MEA). This cell tracks the international processes that affect national policy making. The National Information Board (NIB), a policy making body for cybersecurity, operates independently and is chaired by the National Security Advisor.

- **PSYOPS.** An increasingly vital tool of MDO as finally leaders and the people are the decision makers. It is recommended that strategic PSYOPS for security and military purposes will mainly be dealt at the PMO, NSA, CDS and service HQs level with valuable inputs from

11 India to have Defence Cyber Agency in May; Rear Admiral Mohit to be its first chief; Asian News International dated 30 Apr 19 and numerous national mainstream media

all concerned Ministries (mainly MEA, MHA, MoD, I&B, Science and Tech, Aviation etc) and Intelligence Agencies. Execution will be left to field formations/units (in all domains, not just armed forces) overseen centrally or by Mission Control based on task.

Armed Forces Reforms

As stated earlier our Government and Armed Forces has already begun the process of reforms by way of creation of DPC and CDS who has a three-dimensional charter, giving him a pivotal task of implementation of the process. The charter of CDS is not being elaborated upon which in itself if allowed to be actioned is a major reform and concrete step towards civil-military integration, military structural and organizational reforms, push towards indigenization and pragmatic PPP, economic powers and reforms, and impetus and prioritization to modernization. Focus on growth of IAF and IN, re-structuring, right sizing, planning and creation of integrated theatre forces are other major strategic goals. There is an absolute necessity of clearly established chain of command, control and communications and necessary authorities and permissions to operate in competition and rapid transition to conflict effectively. All three Services and IDS have clearly outlined their mandate of preparing for Grey zone/MDO and are working on creating/adapting structures towards it.

Based on the NSS and NMS promulgated by CCS and NSA/ CDS, the CDS and PCCOCS (Permanent Chairman, Chiefs of Staff Committee) should prepare Conflict Prevention including Deterrence, Conflict Management and Conflict Termination Strategies.

Develop Multi-domain Rapid Response Mechanism. There is a requirement of a central cognitive/non-kinetic operations centre (NKOC) where all information is collected, collated, planning and decision making is taken and loop is completed where ‘after action effect’ is analysed and the circle continues. Staff for the NKOC starting from NSCS (will provide inputs to the CCS and DPC) and PCCOSC will be a mix of military, bureaucracy and core domain experts. At the Services MO and Theatre level it can be tri-services manned. At Army Corps and Divisional level we can have Col GS (NK) and/or GSO 1 (NK) who will be in charge of non-kinetic domains. Advisors from other Arms and Services like engineers,

signals, EW, PI will get linked from within the HQs. The important aspect is to institutionalise the process so it becomes an integral part of operational planning, which will happen due to the changing dynamics of security and conflict. PSYOPS will be directly under the Commander and his chosen staff while execution is left to specifically tasked formations/ units/sub-units (including cyber and IO units).

Re-structuring of Army Formations capable of MDO initially up to Operational /Corps level and moving down to brigade task force (BTF) level. The Corps should have tri-services asset capability with appropriate tri-services representation, and MD capable staff with intrinsic and external resources. Like an Infantry Division apart from its kinetic primary role and support from the IAF, should be able to call on even naval (depending of area of operations) and other operational fires (artillery, communicaions, cyber, psychological) from neighbouring and superior formations.

Integrated Logistics Management. Establishing precision logistics that provides a reliable, agile, and responsive sustainment capability necessary to support two front conflict, rapid power projection (regional power aspirations), MDO, and independent manoeuvre from our strategic depth area to the adversary's depth areas. Formulation of modernised Unified Logistics Structures under a single logistician as Commander. These structures shall be networked and automated for 'Just in Time' supply. This shall be in concert with our overall upgradation of operational logistics infrastructure especially for independent/ isolated sectors. This structure will be better prepared, oriented, trained to combat both offensive and defensive grey zone operations.

Raising of Information and Cyber Operational Units/Sub Units. Cyber and Information operations are increasingly gaining pivotal game changing roles and as an immediate step, similar to EW units and sub units at Service HQs, and integral to Theatre and Operational (pivot and strike corps) formations, we need to raise IO and Cyber units to carry out plg, tasking and execution of offensive and defensive operations. Pro-active actions in both domains will provide exponential gains at the national to tactical levels, and defensive operations can protect us from highly destructive/damaging adversarial operations. US, Russia, China and many modern armed forces have these units in their orbats

for decades. Without going into their role and tasks, one can state that in todays 24X7 Grey Zone environment they are an operational imperative. A battalion at the Service HQ level with a coy at theatre and corps level ab initio with expansion based on experience and operational necessity. I can visualise their role, and it will not be a surprise to observe that they will turn out to be the busiest units during peace and up to confrontational stage, with stepped up role during actual conflict (as can be seen by the activity level of staff and units on cyber and IO specially active theatres like Northern and Eastern Command).

Serious consideration needs to be given to creating basic corps for IO (Information Operations), IW (including EW), Cyber, PSYOPS, Space and Strategic Forces by grouping of similar fields (need not have basic corps individually but similar functional and interrelated fields can be grouped)[12]. This will ensure clear career growth prospects, meet HR aspirations and optimize officer and soldier HR management. Here, we have the option of creating a tri-services IO Corps ab initio which will be a very complex process given the lack of jointness as also diverse IO requirements. It has great advantages as intrinsically IO are essentially tri-services specially at the strategic and operational level, and in future too MDO will be joint operations. Second option which is more pragmatic and implementable is to create individual Service oriented IO Corps. At tri-services, operational and training structures like ANC, IDS, NDA, CDM, tri-services war centres and command posts (CPs), manning norms should be on pro rata basis as hitherto fore. We need not carry this out in haste but carry out dynamic planning after observing how the systems and operational synergy can be optimized.

Military Operations Other Than War (MOOTW). The Armed Forces will continue to meet its other secondary obligations like Aid to Civil Authorities, Humanitarian Assistance and Disaster Relief (HADR), Internal Security Duties, Nation Building, UN Peace Keeping Operations and Out of Area Contingency (OOAC) tasks, including assistance to Friendly Foreign Countries (FFCs) and assistance in 'Non Combatant Evacuation Procedures'.

12 'Organisation and Structures For IW and Influence Operations in Indian Context' by Lt Gen PR Kumar (Retd) for Feb 19, Synergy Magazine Journal of the Centre for Joint Warfare Studies (CENJOWS).

Special Forces Division under the PCCOSC. It will provide unique and empowering Grey Zone warfighting potential. Special Forces shall be equipped, structured and trained to ensure their application in multiple employment opportunities for exponential gains, to achieve our political and military objectives. Their equipment profiling, standards of training and employment strategies must form a vital component of our overall deterrence capability, both in grey zone/ conventional domains.

Force Projection Capability. India's role as a regional security provider mandates a force projection capability to further our national security objectives. A Rapid Reaction Force comprising Integrated Battle Groups with strategic lift and amphibious capability will be an imperative for force projection operations.

Grey Zone Operations in Dense Urban Environment. Build capacity and capabilities for dense urban terrain operational environment for both conventional and sub conventional operation.

Human – Machine Teaming. At the core of our future military planning will be the effective integration of soldiers, artificial intelligence (AI) and robotics into war- fighting systems that exploit existing capabilities for success in battle. Increase in operational effectiveness due to technological development in all fields will be offset by corresponding optimisation.

Training[13]. Integrated services training, exercises and operational discussions to promote jointness and grey zone/MDO as a way of life. Training must be in sync with the front/ theatre threat assessment with emphasis on imbibing technologies being introduced. The focus of training will be as per formation's role with emphasis on 'offensive defence', inter theatre mobilisation, rapid application of strike/ reserve formations, innovative employment of Special Forces and forward logistics management in a techno-centric environment. Reorganising and restructuring training institutions for multi domain multi service multi discipline training after basic training is a daunting task which appears impractical for now and may not even be necessary. Most

13 Ideas from 'Land Warfare Doctrine-Indian Army 2018' accessed on the net on 08 Jan 20; and 'Multi Domain Warfare in Indian Context', USI National Security Paper 2018, by Lt Gen PR Kumar (Retd)

live training could still be accomplished at the unit level in the training areas appropriate to the operational domain. Simultaneously at the operational level, exercises could be linked to provide a situation or common operational picture to an organisation playing the role of the superior HQ with staff. Our Army Command War Centres are ideal for this task, which can graduate to the Integrated Joint Command War Centres. The computer-generated and simulated scenarios fill in the gaps created by resource limitations. The distances and connectivity issues inherent in this type of training would be very similar to actual challenges of geographically separated force employment. This will require the development of leaders able to exercise 'directive style' of leadership. Training staff need to be supplemented from subordinate commands at these joint war centres. This staff training would also build the relationships between Services. Joint Tri Services War Centres will meet the operational requirement, bring synergy and optimise manpower specially of the officer cadre, always in short supply.

Re-structuring of Army HQ. Strike and pivot formations, creation of brigade task forces, appointment of DCOAS (Strategy)[14] with DGMO, DGMI, DGPP and newly created DGIW (both PI and IW) reporting to him will enhance our capability for Grey Zone/MDO.

Conclusion

Living in a world of persistent engagement, calls for capabilities and capacities to fight in the Grey Zone in a multi-domain environment. This requires adoption of a shared war fighting philosophy across the Services (and the Government). Changing a Service's war fighting philosophy requires time and a shared vision across layers of successive leadership across all Services[15]. Initiation of the whole process will need approval and cooperation of multitude of agencies to include Services, the establishment and other security and domain actors. Leaders at

14 Defence ministry approves information warfare branch for Indian army' by Shaurya Karanbir Gurung, The Economic Times, 09 Mar 19; army/articleshow/68329797.cms?from=mdr&utm_ source= contentof interest &utm_ medium=text&utm_campaign=cppst

15 'Multi Domain Warfare in Indian Context', USI National Security Paper 2018, by Lt Gen PR Kumar (Retd)

each level must embrace the concept to provide the organizational, intellectual, and cultural space to establish and evolve the new tenets of competition and confrontation. A foundational joint education rather than a Service-flavoured learning experience may be a more professional approach. A common educational experience will develop a better understanding across the Services of how to operate in the MD construct. In view of our adversarial relations with China and Pakistan, relations with our immediate neighbours needs to be carefully balanced and cultivated to ensure a peaceful friendly strategic neighbourhood. Taking a cue from the US NSS document one can say that 'experience suggests that the willingness of adversaries (read China and Pakistan) to abandon or forgo aggression depends on their perception of India's strength (specially our Grey Zone warfighting capability) and the vitality of its alliances'. Very pertinent to mention that we need to safeguard our maritime, space and information domain and develop a strong maritime presence commensurate with our maritime ambitions and strategy.

The great powers including modern militaries are still finding their feet to organize themselves to conduct future confrontation and conflict in the Grey Zone. Our security environment, modern technology, coupled with new confrontation and conflict methodologies calls for a transformation of our security architecture and Armed Forces to adapt and dominate the strategic space as a regional power. Urgent organisational reforms is a mandatory step for our Armed Forces. This requires vision, leadership (strategic to tactical), moneys, backing of the polity, bureaucracy, and people, indigenisation (make in India), focus, determination, creation of a new culture of integration and jointmanship for MDO and most important of all TIME. The good news is that due to our unique security challenges, history, geography and topography, awareness and intention to adapt and transform our security architecture and Armed Forces is demonstrably visible. India must continue building capacity and capabilities to compete and confront in a MD security environment by operating in the Grey Zone to reach its destined place in the comity of Nations.

***Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd)** is a leading Defence Analyst and a well known Author

GREY ZONE WARFARE IN THE INDIAN CONTEXT- BUILDING CAPABILITIES

Lt Gen (Dr) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)*

Prelude

"In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template."[1] Recent happening globally, like the aftermath of the Arab Spring, portray that prosperous nations can suddenly be engulfed and deteriorate into never-ending war zones, with utter chaos. There are no given rules of war of the 21st century. In fact customary definition of war that imagined violence, armed hostility and active military operations between nations (or with non-state actors), has been immensely enlarged and transformed. Surreptitious, non-contact or non kinetic means of achieving political goals have found acceptance, and exceed the power of military means. The applied methods of conflict have altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures — applied with the power of protest of the population. These can be supplemented by espionage, subversion or use of Special Forces, like the "little green men" - the masked soldiers of the Russian Federation in unmarked green army uniforms and carrying modern Russian military weapons and equipment, who appeared during the Ukrainian crisis of 2014.

The era of information warfare has been singularly influential in diffusing and subsuming war and peace. Hence, the lexicon 'grey zone' warfare emerged in the US, to exemplify the wide chasm between

1 Gerasimov Valery, The Value of Science in Anticipation: New challenges Require Rethinking the Forms and Methods of Warfare, 31 June 2014, accessed at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

war and peace. The International Security Advisory Board of the US Department of State included the following in the grey zone conflicts:

- Cyber, information operations, efforts to undermine public/allied/ local/ regional resistance, and information/propaganda in support of other hybrid instruments;
- Covert operations under state control, espionage, infiltration, and subversion;
- Special Operations Forces (SOF) and other state-controlled armed units, and unacknowledged military personnel;
- Support – logistical, political, and financial – for insurgent and terrorist movements;
- Enlistment of non-governmental actors, including organized criminal groups, terrorists, and extremist political, religious, and ethnic or sectarian organizations;
- Assistance to irregular military and paramilitary forces;
- Economic pressures that go beyond normal economic competition;
- Manipulation and discrediting of democratic institutions, including electoral system and the judiciary;
- Calculated ambiguity, use of /covert/unacknowledged operations, and deception and denial; and
- Explicit or implicit threat use, or threats of use of armed force, terrorism, and abuse of civilian populations and of escalation.[2]

It is instructive to read the explanation of grey zone conflict in the ISAB Report, that, it '…denotes the use of techniques to achieve a nation's goals and frustrate those of its rivals by employing instruments of power –often asymmetric and ambiguous in character –that are not direct use of acknowledged regular military forces."[3] It becomes apparent

2 International Security Advisory Board, US Department of State, 03 Jan 2017, accessed at https://2009-2017.state.gov/t/avc/isab/266650.htm

3 International Security Advisory Board, US Department of State, 03 Jan 2017, accessed at https://2009-2017.state.gov/t/avc/isab/266650.htm

that ambiguity, irregularity and unconventionality of warfare become the capstone of prosecuting under the larger ambit of Grey zone warfare, while the threat of use of force may manifest itself to a conventional war, subsequently.

The 'grey-zone' in Indian context can be taken as state of being between war and peace, where adversaries aim achieve geopolitical or territorial ends without overt military aggression and crossing the threshold of open warfare.[4] Contextually today, the toolkit for coercion below the level of direct warfare includes information operations, political coercion, economic coercion, cyber operations, proxy support, and provocation by state-controlled Forces.[5]

From fake news and online troll farms to terrorist financing and provocating the disillusioned, the inimical approaches often lie in the contested arena somewhere between routine statecraft and open warfare—the 'grey zone.' For the purpose of this paper, the concept of grey zone is taken as between war and peace, from routine state craft to short of conventional war. The central theme this paper propounds is that with two adversarial neighbours, India may well be in the throes of grey zone warfare in many manifestations. There is an optimal necessity to create capabilities to fathom the subtleties of the character of this type of warfare and plan to combat it with vigour.

Pakistan and China: Grey Zone Operations against India

In contemplating Pakistan's grey zone strategy, the relevant approach can be described as "… to reap gains, whether territorial or otherwise, that are normally associated with victory in war." [6] Pakistan without crossing established red-lines and exposing itself to the penalties and risks of escalation to conventional war, is attempting to reap success by

4 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

5 Grey Zone Project, CSIS, 13 Aug 2019, accessed at https://www.csis.org/ greyzone

6 Hal Brands, 'Paradoxes of the Grey Zone, Foreign Policy Research Institute, 05 Feb 2016, accessed at https://www.fpri.org/article/2016/02/paradoxes-grey-zone/ on 29 Dec 2019

utilizing proxies. The decade gone past has greatly enhanced the toolkit of information warfare for Pakistan– from ingenuous disinformation and propaganda to taking advantage of social media for faster dissemination, from fanning radicalization to civil unrests. The realm of information battlefield has provided plausible deniability to Pakistani establishment. It is typical of Pakistan to be vigorous and aggressive in using strategic communication, and in doing so deliberately remain well under the threshold of conventional military conflict.

The breadth of this anti-India grey zone warfare emanating from Pakistan is fairly wide, and not only related to disinformation and incitement. It also remains a low-cost option. There is calculated pushing in of fake Indian currency notes (FICN), drugs, hawala money, cyber warfare, raising varied bogeys at international fora, fanning internal dissent, to sponsoring terrorism by using proxies. Jammu and Kashmir is but one of the manifestation of the larger geo-political rivalry with India. Exploiting social media and technological tools and cyberwarfare, adverse information dissemination, with fakes/ deep fakes/ use of dark web and distortions is continuous, without any challenge of attributability. Cumulated with this is terrorism, from Mumbai, Pathankot, Uri, Nagrota to Pulwama. There is a very large strategic canvas created by Pakistan, to undermine Indian national security. This multi-prong offensive against India is retained below the threshold of conventional war in an ambitious grey zone campaign. India, by itself is a large and most diverse nation, with a never-ending cacophony of voices and myriad problems which provide incalculable opportunities that a belligerent and adversarial Pakistan can and does easily take advantage of.

China is the master of grey zone ambiguity. Henry Kissinger had opined that, "…whereas Western tradition preferred the decisive clash of force, emphasizing feat of heroism, the Chinese ideal stressed subtlety, indirection and patient accumulation of relative advantage."[7] Sun Tzu had centuries ago prophesized that 'all warfare is based upon deception.' Psychological operations that would end in intellectual confusion to the adversary are part and parcel of the Chinese philosophy. The 'Unrestricted Warfare'[8] nullified the boundary between battlespace and

7 Henry Kissinger, On China, Penguin Books Ltd, London, 2012, p47.

8 Qiao Liang and Wang Xiangsui, Unrestricted warfare, Beijing,1999, accessed at

non-battlespace, with non-military methods including, trade, economic aid, resource, financial, ecological, network warfare and the like. The three-warfares strategy is a form of state craft, that encompasses non-kinetic means to achieve political ends. The first of the three-warfares is psychological that seeks to influence and/or disrupt opponents decision-making capability, create doubts, foment anti-leadership sentiments and diminish the will to fight. The second, media warfare, also called public opinion warfare, is a constant ongoing activity aimed at the long term influence of perceptions and attitudes, leveraging all instruments that inform and influence public opinion. And the third, legal warfare or lawfare, exploits the national and international legal system to achieve political and commercial objectives.[9] As one delves into and analyses the three-warfares, it is apparent that though military coercion may be part and parcel of the overall conceptology, political aims are achieved largely by manipulation and economics.

In case of China, Sun Tzu's philosophy of 'subduing the enemy without fighting' is at play. China has consistently demonstrated preference for ambiguity, risk manipulation and controlling the narrative to win without fighting.[10] China astutely utilizes the three-warfares strategy in the ambit of grey zone warfare against India.

Its strong reliance on legal and narrative rhetoric on the boundary question, without even pitch-forking its views in exactitude, intelligently obfuscates the realities and ties any contemplation into knots. The management of transgressions on the Line of Control is lesser an attempt to change status quo by force, more of intelligent coercion to keep the pot boiling and tie India down in perpetual state of anxiety. Added to it are the underpinnings of an ever-burgeoning trade deficit. Again, internal developmental issues in India do provide it with fodder to undertake focused information warfare. These are all harmonious with the age-old foundations of Chinese strategic thinking. The philosophy, '…if object of war is to acquire resources, influence and territory, and to

https://www.cryptome.org/ cuw.htm

9 Stephan Halper (ed), China: The Three Warfare, Washington, DC, Office of Net Assessment, Office of the Secretary of Defense, 2013, p12.

10 Oriana Skylar Mastro and Arzan Tarapore, 'Countering Chinese Coercion the Case of Doklam', War on the Rocks, 29 Aug 2017, accessed at https://warontherocks.com/2017/08/countering-chinese-coercion-the-case-of-doklam/

project national will…China's Three Warfares is war by other means,'[11] is absolutely tailored against India. It has also been argued that China's grey zone strategy has been in play along the Indian borders. It has involved the Chinese military bringing ethnic Han pastoralists to drive Indian herdsmen from the traditional pasturelands and opening the path to salami slicing through subsequent PLA patrols.[12] The Chinese repertoire of offensive tool-kit hence includes communication campaign, artificial intelligence (AI) and cyber warfare. Its extensive use of proxies, covert means and information domain can create a false narrative that can become detrimental to national security.

Strategising for India – Building Capabilities

A question that begs answer here is whether or not a grey zone war can be fought with our present national security formulations? In such context, how does a nation like India deter grey zone warfare and formulate its national and military strategy?

Conventional Indian concepts of war are incompatible and fundamentally skewed from the realities of grey zone warfare of the twenty-first century. Indian adversaries have mastered creation of an adverse narrative and use advanced technologically to embrace this newer form of warfare. It must hence be expected that in future, the conflicts that India will have to face (or is facing even currently), will necessarily and largely be a grey zone warfare with adversaries utilising psychological, economic, political, and cyber realms. In this political, religious, regional, social and cultural identities that are fanned and pitted against one another create cleavages. Increased confusion and disorder will ensue when weaponized information abetted externally against India, would create insecurities in the populace.

India, hence, must then develop framework of strategic deterrence against weaponized information, finance, cyber and other subversive forms of aggression – against the adversaries. A 'one size fits all' national security policy would not be effective. While salience and preparations for

11 Stephan Halper (ed), China: The Three Warfare, Washington, DC, Office of Net Assessment, Office of the Secretary of Defense, 2013, p12.

12 Brahma Challaney, 'China's Salami-slice Strategy' The Japan Times, 25 June 2013, accessed at https://chellaney.net/2013/07/26/chinas-salami-slice-strategy/

modern conventional, kinetic war cannot put on back-burner, accepting that a grey zone campaign against India may be ongoing or planned for, is critical. Hence a joint multi-domain specialisation would indicate right preparation for future warfare. That is the responsibility on the shoulders of today's political and military leaders. Seven key postulations for preparing India for grey zone warfare are proffered:

- Grey zone warfare as per definition and ambit describes domains that can well be termed as largely non-military. Hence the prosecution of non-military domain aggressive actions by an adversary would cause damage or destruction to national infrastructure or socio-economic foundations of the nation. India must take externally abetted such actions as acts of war – even if the adversary is unidentifiable, un-provable or resorts to plausible deniability. Cases in point would be cyber attack on national infrastructure, power grid, banking system, and the like. War hence in a grey zone may be a permanence state – and must not be imagined as a territorial contest. This might seem unduly alarmist, and may affect rationality. However, the new character of war has its dictates and strategizing for the same is imperative. India needs to redefine war and warfare, as even manifestations of grey zone in non-military domain, would hurt the foundations of the nation.

- Since grey zone is not in exclusive military domain. Defensive and law enforcement capabilities in India symbolized by NSG, NTRO, National Cyber Coordinator, intelligence agencies, Central Armed Police Forces and State Police require parallel developments, which need to be skillfully fused in a specifically tailored National Security Structure. A National Counter Terrorism Centre (NCTC) has been on the anvil for sometime, is a necessity, linked with the National Intelligence Grid (NATGRID), and other law-enforcement and intelligence agencies. Grey zone warfare necessitates intensive consolidation of all resources and security assets available with various infrastructural agencies, without resorting to any battle of the turf. The challenge is to plan development of offensive and defensive grey zone warfare technologies and expertise. India, with the large challenges is a right arena for an apex Internal Security organization (like the US Homeland Security) – which has requisite data bases and analysis mechanisms. The domestic security organizations above, and indeed, security organizations of disaster relief,

medical aid services, power grid and water/river/canal management, banking systems and share markets, rail and metro services, airports authorities, and first responder mechanisms should become sub-sets of the Apex Organisation.

- If war is the continuation of politics "by other means," (Clausewitz), social networks tend to continue politics by additional means, to influence susceptible people. As has been seen in India, this creates new, dangerous predicaments that mandate preparations. Indoctrination or causing cleavages in the society by social networks is not cyberwarfare (which uses the internet to attack and disrupt networks). A multi-prong and concerted effort is necessary to this ever-expanding stream of diatribe. We need much better public-private cooperation, and ensure that networks like Facebook, Twitter and WhatsApp establish permanent monitoring systems and liaison with Department of Internal Security to assist them in responding/ taking cognizance of threats in real time. There ought to be legal incentives and punitive actions for social media networks for compliance.

- Psychological warfare, fake news campaigns, propaganda, subversion, intimidation, demoralization and the like, are common place in India. State and non state actors are weaponising information, to the advantage of adversaries. These will become permanent features. The case in point is Cambridge Analytica, and the influence pedaling in the last US Presidential Elections. It is not that psychological warfare and propaganda is a new realm, however the media (including social media) have multiplied manifold, its techniques are being made sophisticated, and the effect it is having on populace is credible. Psychological warfare is leading to increasing radicalization and needs to be addressed pronto by parallel streams of well planned counter-radicalization and information management plan. Naturally, these are also grey zone threats, ones that seem perfectly benign, but which has immense potential to address the collective psyche of the peoples of a nation. Narrative Warfare and influence operations is another realm that India needs to venture into, to generate long term narratives for the nation. We also require countering adverse narratives by adversaries – a continuous stream of adverse propaganda – by focused plans. For this there is need of conjoined team of experts like social psychologists and media/ social media experts,.

- India is a diverse and developing nation and an aspirational society that is prone to internal protestations. There is need to build sentiment analysis system to continually analyse societal anxieties. This sentiment analysis should be a process of extracting opinions within the nation that have different schisms - positive, negative or neutral. With the help of sentiment analysis, we will be able to collate nature of opinion that is reflected in documents, websites, social media feed, etc. Sentiment analysis thence can be used to monitor and analyse social phenomena, for spotting of potentially dangerous situations and determining the general mood of the society. Several software companies have developed proprietary text mining systems for data visualization, and researchers have developed expert systems for sentiment analysis. In the diversity that is India, such detailed analysis will facilitate influence operations or counteract on potentially difficult situations.

- Military conventional deterrence remains fixated on all-out or limited high end conventional war that remains within the ambit of state versus state warfare. In case of India, conventional military superiority with the threat of deterrence by punishment is insufficient to force adversary to cease proxy war or grey zone operations. This credence requires serious rethink. The likelihood of strong conventional kinetic response to a hybrid non-kinetic attack or protracted grey zone campaign must not be negated. The quid pro quo response to any form of grey zone operations may emanate in a totally different realm. The issue created by the hybridization of threats opens new vistas in deterrence debate and response options, and mandates further analysis. Suffice it to say that strong conventional force will be inadequate deterrent against grey zone warfare. Hence proportional or disproportionate response cannot be predictable and will be contingent on national will and political intent at that juncture. India will require an effective bouquet of quid pro quo hybrid options, a quiver full of variable arrows that can be selectively employed, as stronger deterrence.

- The challenges of strategic cyber weaponry with adversary's malware embedded browser hacking or hardware trojans that export data unfettered, or are sleepers that can be activated on call, are dangerous portends for national infrastructure. Such cyber challenges are growing exponentially. In critical infrastructure equipment and

software must be sanitized and detection systems planned for existing systems to thwart inimical designs against the nation, or we may face as is often termed Cyber Pearl-Harbour! India has the potential internally to establish expertise for an effective defensive cyber defence, and must be undertaken on war-footing.

Conclusion

A linear conventional conflict is a declaration of war formally, and will be sequential in progression of a planned strategy. A grey zone campaign involves simultaneous deployment of multitude of non-military warfare methodologies, in peace, supported by irregular, cyber and informational warfare tactics, aggregated together or used in disaggregated form. The definitional and terminological structure of grey zone warfare has confused warfare itself. Any rational consideration of this plethora of these threats, and planning for combat is well nigh impossible, as many of them are indeed faceless. The kind of toolbox necessary to combat them is unimaginable in content. However, for an adversary as dogged as Pakistan, grey zone warfare with its myriad manifestations is God-send against India. The long strides that China has taken technologically, its vast export of electronic and cyber equipment to India and the apparent collusion with Pakistan, makes India particularly vulnerable. In this undeclared grey zone campaign, any adversary would attempt to exploit nation's vulnerabilities, fault-lines, social divides and cohesion.

The adversarial use of grey zone campaign also makes India defensive on international fora and internally causes disruption that strains national governance and ties India down in internal dissensions. India needs to get the act together, as the grey zone threats are not linear territorial threats, these target the nation wholesomely, and have the capacity to hurt. In managing these threats, one of the most significant problems in India (as is elsewhere too) is the battle of the turf. We need an Apex Organisation akin to US Homeland Security that obliterates the turf-battles, fathoms the threats, and creates capabilities to address them. It also mandates a societal approach!

***Lt Gen (Dr) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)** is a former AG and GOC 14 Corps. He is currently Distinguished Fellow with Centre for Land Warfare Studies

THE MANY SHADES OF GREY: COUNTERING AND EXPLOITING GREY ZONES AT SEA

Rear Adm SY Shrikhande, AVSM (Retd)*

"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."

Abhijit Singh[1]

"Grey zone activities arguably have a history almost as long as organised activity at sea."

Rear Admiral James Goldrick[2]

Between Black and White: a History as well as a Future for the Grey Zone!

A simple way of describing the grey zone is to think of it as 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."[3] Another way to look at the matter is to think of what someone does in the grey zone as warfare in the pursuit of some objectives of strategy. Thus, if we think properly of war as being at only one level, the strategic level, and warfare having three levels, the strategic, operational and tactical, then understanding grey zone warfare in its tactical and operational

1 Abhijit Singh, 'Deciphering Grey-Zone operations in Maritime Asia', *ORF Special Report #71*, 01 Aug 2018

2 James Goldrick, 'Grey zone operations and the maritime domain', *ASPI Special Report*, Oct 2018, ISSN 2200 6648.

3 Abhijit Singh, *ibid*. He takes this description from an article by Green, Hicks, et al, 'Countering Maritime Coercion in Asia', *Centre for Strategic and International studies*, Jan 2017.

levels becomes easier to understand.[4] Chorn and Sato describe grey zone (note that the Americans spell it with an "a" in grey) thus:

> "Grey zone tactics, often used in the realm of asymmetrical or hybrid warfare, are defined as an 'effort or series of efforts beyond steady-state deterrence and assurance that attempts to achieve one's security objectives without resort to direct and sizable use of force.' They can include a mix of conventional warfare, irregular warfare, and cyber warfare with other influencing methods, such as fake news, diplomacy, lawfare, and foreign electoral intervention. Through grey zone tactics, potential adversaries can inconspicuously coerce their targets to serve their interests while avoiding the possibility of large-scale conflict."[5]

The grey zone, therefore, has a wide spectrum that also deploys what we understand as the DIME (diplomatic, informational, military and economic) instruments. Within this framework, the Chinese articulation of "three warfares" also fits in.[6] In fact, history shows that neither grey zone operations, nor hybrid warfare (terming it hybrid war is somewhat problematic), nor "three warfares" are actually novel or new. Of course, in their tactical measures and potential for greater future use, the Chinese have perhaps been more imaginative, proactive and relatively more prolific than anyone else in the present times. Given their essential timelessness, we could, therefore, consider three inferences of grey zone warfare for elaboration:

4 This writer is working on the assertion that war does not have three levels, the strategic, operational and tactical. It is warfare that is at three levels. This is not mere semantics because as several wars have shown, competence and even significant successes at the tactical level do not automatically lead to victory. Military victory at War's strategic level is important to achievement of some objectives at the political level of strategy, but not in its entirety. Many scholars still write about levels of war, but perhaps this is not a useful way to consider the issues.

5 Adrian Chorn and Monica Michiko Sato., 'Maritime Grey Zone Tactics: The Argument for Reviewing the 1951 U.S.-Philippines Mutual Defense Treaty', *CSIS,* 01 Oct 2019, https://www.csis.org/maritime-grey-zone-tactics-argument-reviewing-1951-us-philippines-mutual-defense-treaty

6 Larry M. Wortzel, 'The Chinese People's Liberation Army and Information Warfare', *Strategic Studies Institute*, US Army War College (March 2014), 29.

- Historical examples for operations in the grey zone abound.[7] It has had a complex and consistent past and shall have a future as well.

- Such 'warfare" should not be seen primarily as something that nations like China (from India's perspective as well as that of several nations across many longitudes) or Russia (mainly from the West's perspective) engage in.[8] As a corollary, neither should it be seen from the limiting lens of being a weapon of the weak against the strong. It is more complicated than that.

- Therefore, operations and tactics in the grey zone could also be options-- for lack of a better phrase—that the "good guys" could continue using. This is in line with the very beneficial idea of winning something, or shaping something or preventing something without any, or hardly any, fighting.

Reaching Back into History & Relating it to Current Contexts

Some facets of the Russo-Japanese War of 1904-05 had both belligerents and neutral China operating between the black and white of conflict and peace. Russia and Japan essentially fought over control of China, especially Manchuria and for mastery of the sea. Russia was mightier and a European power as well. China, the sufferer at the hands of both, declared neutrality. As Elleman says, "China's policy of neutrality was left intentionally vague from the beginning to give the greatest range

7 Goldrick, ibid. He cites not only recent examples of grey zone tactics, but also the "Cod Wars" between Iceland and the UK between 1958-1976; the so-called first Paracels war in which China took over these islands with force from south Vietnam in the closing days of the Vietnam war and with the Americans having effectively lost the war against north Vietnam; issues over Gibraltar between Spain and the UK, and so on. These are important examples of the problems and perhaps utility of grey zone operations.

8 Much of today's work on grey zone warfare is centered around what China and Russia are doing. These are of course, good examples, but the spectrum and players are beyond these two large powers. For example, see Ross Babbage, 'Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West can Prevail', *Center for Strategic and Budgetary Assessment* (Washington DC, 2019).

of action to all the interested powers. Often the undefined nature of the China's neutrality led to divergent interpretations of international law and diplomatic practice."[9] What initially surprised Japan was the disruption Russian ships caused its trade interests due to interdiction of vessels by so-called Russian "volunteer ships." This was done as far away as in the Red Sea. Russia declared coal as contraband of war and began intercepting ships carrying British coal to Japan. Elleman points out in this case study that, while the quantitative disruption was somewhat limited, insurance rates went up for all; there was fear of escalation of Germany stepping in on Russia's side and England on Japan's as a treaty partner since 1902.[10] Goldrick similarly points out the impact on insurance, re-routeing, change of ports and so on, while remaining in the grey zone with some countries.[11] China interpreted neutrality quite broadly, interning Russian ships in a way that favoured Japan at times, yet putting up with the Japanese Navy's active intervention within territorial waters against Russian ships and their crews. The deeper inference is that neutrality can be loosely interpreted; that it could effectively be exploited by the adversary; that what we call "maritime militias", ELINT trawlers and merchant ships with changing characteristics are all still grey zone possibilities. Add to this are factors of a reluctance to escalate and to try and operate within the grey zone. Notably, while Imperial Japan did not have a navy or bases that could support it in and around the Red Sea, it leveraged to an extent the rivalries between European powers and its relatively young alliance with Britain. It shouldn't be forgotten that Britain was also a major exporter to Japan, including for modern military hardware; it was also a lender and investor. Today's China has bases and places, some friends and power as a P-5 member of the Security Council as well as real clout in most parts of the Indo-Pacific. It is today's Britain to a few Japans in the Indo-Afro- Pacific region. It is also better placed to flex its muscle while trying to remain in the grey zone.

There is more. KM Pannikar, the well known Indian maritime strategist-historian, perhaps described the complexities of grey zone operations and benefits for some in analyzing the Vasco-da Gama epoch.

9 Bruce Elleman and SCM Paine, *Commerce Raiding: Histrorical Case Studies, 1755-2009*, Naval War College Newport Papers #40, Oct 2013, 121.

10 Elleman, 122-125.

11 Goldrick, 5.

In line with concerns voiced by Goldrick about "freedom of navigation" (FON), Pannikar describes that in the early 16th century Indian Ocean, Portuguese admirals and captains quite widely enforced their King's right to be the "Lord of Navigation." He adds that "After the Egyptian admiral Mir Hussein's departure from Indian waters in 1509, the Portuguese proceeded to enforce this claim…Any ship sailing without their *cartas* was treated as a pirate and liable to capture and confiscation."[12] Enforcement of such restrictions was not only dependent on what could be legitimately seen as Portuguese naval ships, but outsourced to merchant ships as well. A part of earnings from such extortion went into Royal coffers and some to the enforcers. Indirectly, it enabled a monopoly on trade. Pannikar sums it up well: "Whatever the admirals of the Zamorin might do in the coastal waters of Malabar, India's trade was theirs and there was no one to question it…"[13] It is a moot point that if the few Indian coastal kingdoms—even if not the somewhat sea-blind Mughal kings in Delhi-- had put together a few privateers, at the least the monopoly would have been contested to an extent. No one really had any organised system of '*little blue men'* as some call the modern Chinese militia operating in the South China Sea. [14] Of course, much has been written about the Chinese use of layered forces that increase options for them and complicate matters for others. An interesting view on the advisability of a 'maritime militia" is by India by Rear Admiral Monty Khanna. Keeping in mind the grey zone in which threats arise, as they did in the state-sponsored and abetted terror attacks on Mumbai in Nov 2008 ("26/11"), he recommends some corresponding countermeasures. [15] Essentially these replicate what the Chinese maritime militia is organized, trained and tasked for through more formal incorporation of the Indian fishing community into the defensive architecture of coastal security. In the Indian context, given our very fortunate democratic

12 Pannikar, *A Survey of Indian History,* Popular Press (Bombay, 1964), 186. Also, Goldrick, ibid.

13 Pannikar, 187.

14 The term 'little bluemen' derives from 'the little green men' used for some militias operating in the grey zone during the Russia- Ukraine conflict over Crimea and other issues. For example, see Andrew Erickson, http://www.andrewerickson.com/2015/08/tracking-chinas-little-blue-men-a-comprehensive-maritime-militia-compendium/

15 Monty Khanna, 'It Is Time We Raised Our Own Maritime Milita', *Synodos Paper*, *Vol-XII No-21*/Oct 2018.

system, federal structures and difficulties in central orchestration, the little blue men may not quite have Chinese characterisitics, which is not a bad thing. However, the suggestions he makes are worth considering for India as the "good guys" with experience of what "bad guys" near us have done and can do again.

Lest it be thought that such measures seem attractive only in the developing (or even the "Third World"), Goldrick's analytical summary of the so-called Cod Wars between the UK and Iceland (1958-1976) is quite instructive. A weaker nation, Iceland, bested a much more powerful Britain through better leveraging of DIME. This was done in such a way that a larger Navy had to yield because a fuller conflict was not an option. Iceland's claims of fishing rights in the pre-UNCLOS 3 epoch were not "rules-based" to use a phrase that seems more current. It leveraged information by being faster with stories and images of British belligerence. It won much more of international sympathy than could the UK. Iceland also leveraged its membership of NATO and the location of important air bases by threats of exiting NATO and moving closer to the USSR. It eventually led to the British constructing newer fisheries protection vessels with stronger bows; deployment of tugs that could ram or resist ramming better. Among other measures, it resulted in a class of vessels-- now common-- the Offshore Patrol Vessels (OPV). One may add here that the Cod Wars are a fine illustration of "three warfares" long before it has come to be seen as a novel concept the Chinese created.

With future fishing disputes, issues that may arise out of US and UK difficulties over the legality of Diego Garcia,[16] or persistent instability in the NW IOR/ West Asian sphere with its maritime consequences, perhaps grey zone problems and some grey zone tool kitting may be well-advised.[17] Geoffrey Till gives several examples of skirmishes, rows and violence at sea over fishing, warning that, "competition for dwindling

16 For a different view on Diego Garcia see David Brewster, 'Australia's stance on Diego Garcia dispute is increasingly untenable', *The Lowy Institute,* 11 Dec 2019, https://www.lowyinstitute.org/the-interpreter/australias-stance-diego-garcia-dispute-increasingly-untenable

17 Geoffrey Till, Seapower: *A Guide for the Twenty-First Century*, Frank Cass, London (2004). In the context of the Cod Wars, Till explains that, "By forcing the more powerful to take on international opprobrium associated with the use of force against the weak, a grossly inferior naval power can sometimes make use of political possibilities and even odds against much more powerful forces." (297-298.)

resources may easily spill over into conflict."[18] Is this far-fetched? It is difficult to say, but if the early stages of water-wars in the grey zone are somewhat discernible today, then "fishy" conflicts have occurred for several decades already.

The More Things Change…

The history of warfare, and in a sense of tensions that never broke out beyond the zone between peace and clearly recognisable conflict, demonstrates that some lessons are enduring even if history ought not be templated. In Clausewitzian terms, the nature of war has enduring attributes, even if the character of warfare changes with developments in the instruments and methods of warfare. Therefore, while the likelihood of larger-scale interstate wars may have receded, there are no guarantees that these won't occur. Such predictions have been made in the past! Similarly, we should avoid confounding ourselves that grey zone warfare, or three warfares, or multi-domain warfare and even Hybrid War are recent ideas even if quite a few scholars in the West may have said so. Even smaller tensions and grey zone warfare (GZW) can be multi-dimensional with air, sea, cyber and space dimensions playing some or major roles in combinations. Much of current Indian writing seems to suggest all these "warfares" as novel concepts, and quite new for us. On the other hand, Admiral Khanna's essay explaining that warfare has really been multi-domain for a long time is refreshingly different..[19]

Maritime GZW would continue to have facets that would matter in the Indian context, but one would hasten to add that there is little that is fundamentally unique to our context in most areas of warfare. GZW itself manifests in several ways. Some for us to consider are:

- It has territorial dimensions as has been seen in the case of the South and East China Seas with the potential for more trouble, skirmishing

18 Till, *ibid*., 312-313.

19 See final essay by Rear Admiral Khanna in CENJOWS Compendium in the *Synergy Series* on 'Multi-domain Warfare in the Indian Context', (New Delhi, Feb 2019), pp130-138. His essay is appropriately titled *"Multi domain Warfare: Old Wine in a New Bottle"* and seems to be the one exception that says so with most others thinking of MDW as a new concept. Another example is a paper on hybrid war published by the USI, 'War Beyond Rules: Hybrid War and India's Preparedness, Dec 2018'.

and much more in times ahead. This is not merely related to areas of dispute over maritime boundaries, but of base lines, interpretations of zones and rights within these zones. Some clauses in the Maritime Zones of India Act (1976) are at variance with the UNCLOS 3 that followed and could be contested by other nations more vigorously than at present.

- The use of seas for what could be discernible acts of terrorism, need little elaboration within India.

- Threats to shipping, whether India's or of other nations may become a more severe issue and yet remain in the grey zone. India may be expected to play a greater role, and if we are to be counted as a great power, instead of merely being satisfied with "great presence" then our capabilities to do so will have to match up. [20]

- An increasing danger could be the impact of cyber attacks on naval assets or on shipping as did happen to the Maersk line in June 2017, unsettling not only its operations for a few days but creating a much wider impact.[21]

- Given the lessons of the "Tanker war," which continued as GZW in a sense during the 1980-88 Iraq- Iran war and affected dozens of countries, India included, mines and even missiles need to be seen as maritime IEDs (Improvised Explosive Devices). Pakistan and China both have very large numbers of mines in their inventories as do several other players in the western IOR. Sea mines are, of course, a very permissible weapon of war, and some versions can be made quite sophisticated at a relatively low cost. Secondly, it is conceivable that non-state actors with, or without state-support could also make relatively high-effect mines. They have already used missiles in multiple dimensions. There is not much reason to believe that they couldn't or wouldn't use these against India. On the other hand, India is likely to have a very modest number of mines to be used defensively or offensively in conflict. Perhaps of as much or even greater concern is the declining mine-countermeasures

20 Akshobh Giridharadas*, National Interest*, 'India's role in the Great Power Struggle Over the Indo-Pacific Region', 23 Jan 2020, https://nationalinterest.org/feature/indias-role-great-power-struggle-over-indo-pacific-region-116556.

21 Reuters, 'Maersk Says Global IT Breakdown Caused by Cyber Attack, 27 Jun 2017, https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

capability as commented by this writer two years ago.[22] A scholar has recently reiterated this point.[23]

- Like mines, piracy could be another major GZW concern as it has been until very recently. It could take the form of a more political instrument rather than an economic instrument for plunder as it has primarily been. In fact, navies need to stop addressing maritime piracy as a non-traditional threat because for a fact, it has been one of the most traditional threats that nations and even alliances/ coalitions have tried to combat (and sometimes even leveraged) for over two millennia.[24]

- Refugee crises resulting in influx by sea, akin to what may happen across borders, could create GZ issues because of the possibility of very inimical elements infiltrating as part of a humanitarian issue, creating a nearer-term problem. In the longer term refugees could become part of more intractable political issues for subsequent governments. The use of some force, screening, turning back, interning and so on might all be unpleasant but necessary measures in the maritime domain for the Navy, Coast Guard and other agencies.

- Capable non-state actors, with or without support of some state, would be expected to use instruments within DIME in imaginative ways that more ponderous, conformal and slower to adapt instruments like a Navy or Coast Guard. To counter this, a state's instruments would need to intellectually, tactically and operationally prepare themselves to prevent, respond or initiate actions in the GZ. Our adversaries and their associates could be expected to exploit and leverage air, even underwater, cyber and space domains tactically and operationally. We are going to see more of it, not less.

22 Hindustan Times, 10 Mar 2017, Rahul Singh, https://www.hindustantimes.com/india-news/harbours-at-risk-navy-won-t-have-minesweepers-for-at-least-three-years/story-MOaPuaxqjdFiZItMdSDnHO.html

23 Prakash Gopal, 'India: Navigating the Straits of Capability', *The Lowy Institute*, 23 Jan 2020, https://www.lowyinstitute.org/the-interpreter/india-navigating-straits-capability

24 Even Indian naval doctrinal and strategy documents use the more prevalent category of non-traditional threat for piracy when it is very, very traditional. See, Ensuring Secure Seas: Indian Maritime Security Strategy, NHQ/MOD (New Delhi, Oct 2015), 37-39.

Concluding Thoughts

The above list is long, but perhaps not exhaustive. Yet, a few broad conclusions are possible:

- First, GZW is not new in essence, even if some details and developments may turn out to be new or even novel in terms of events/ instruments/ countermeasures.

- Second, to think of it as a measure that weaker nations or groups may use against stronger ones is not necessarily right historically or in contemporary times. China is *de facto* stronger than anyone else in its own littorals and its power, influence and interests are becoming global.

- Third, operating tactically in the grey zone for some operational and strategic objectives ought not to be seen as something that "bad guys" do against the good. Equally, it is a zone to defend, be offensive as required and exploit to gain objectives by a nation like India. Its maritime instruments are very much part of the architecture but integration and jointness become necessary.

- Fourth, there always has been a grey zone between the white of peace and the black of clearly discernible conflict. The instruments of warfare that are required for fighting across the spectrum of warfare, for the contexts of that period, would be the same that would need to operate in the grey zone. Tactics could be different, of course, and some of those assets and capabilities that are more efficient at the lower end of the spectrum would be more used in GZW.

The Navy's grey hulls or a coast guard's white hulls or little blue men and the myriad types of instruments that come to play in the grey zone all need to be kept sharp and agile in mind as well as matter. It is possible that our adversaries may perceive more shades of grey in the grey zone. However, denying them that metaphorical sea room would be part of our effort to win without fighting, or at least without fighting too much while retaining the instruments and strengths to use full force if and when warranted.

***Rear Adm SY Shrikhande, AVSM (Retd)** is a reputed Defence Analyst and author

AEROSPACE AND GREY ZONE WARFARE

Air Mshl Anil Chopra, PVSM, AVSM, VM, VSM (Retd)*

There are multifarious forms of state activity in the area between war and peace. Hybrid or 'grey zone' conflict between states has been an area of action in recent years. The grey zone is characterized by intense political, economic, informational, and military competition, more fervent in nature than normal steady-state diplomacy, yet short of conventional war. Beyond the nuclear 'mutually assured destruction' the Cold War was a 45-year-long grey zone struggle lased with posturing and intrigues. The make-up of participants in military conflicts is broadening. Together with regular forces, the internal protest potential of the population is being used, as are terrorist and extremist formations. There has been a shift from sequential and concentrated operations to continuous and dispersed operations conducted simultaneously in all spheres of confrontation and in remote theaters of military operations.

Grey zone is battle-space with a steadily growing number of players, capabilities and agendas. Organized crime, state-backed troll teams, terrorists, political activists and IP thieves, are all part of the 'grey zone' conflict. US General Charles C. Krulak coined the term 'Strategic Corporal' in 1999 to imply the large impact a few low-ranking American troops could have in a foreign crisis. After years of conventional air war in the Middle East, American security concerns are turning to a resurgent Russia and China as serious emerging competitors who have begun exploiting the 'grey zone' conflicts to advance their interests at much lower cost and risk. The Russian cyber attacks in Estonia, covert employment of regular Russian forces in Ukraine, Tamil Tiger insurgency in Sri Lanka, and Pakistan supported terror ops in Kashmir are all cases of grey zone warfare. Political machination, covert operations, guerilla warfare, and active measures are now considered part of grey zone conflict.

The range of means being used to project state power is wide. Many grey zone activities are functions of a restructured global economy. The most potent weapons today are information, capital and credit, and were once monopolized by the US and its allies, who also dominated the military power. That is no longer the case. The narratives are in many hands. China is using excess capital and disbursing credit at an unimaginable scale. China has also been indulging in intellectual property theft. Russia is a big player in cyber space. Since the 1960s, only 7 percent of insurgencies and terrorist groups have been defeated militarily, whereas 83 percent of these groups ceased to operate due to policing or politicization.

Grey Zone Warfare Defined

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 that are difficult to achieve with traditional conventional force options. The government on the receiving end usually struggles to confront and limit the aggressors' actions, either because it cannot sufficiently deploy resources due to perceived or real domestic and international constraints or because it cannot effectively counter the aggressor, which purposefully avoids direct confrontations. The 'grey' antagonists wage a subtle war in which they are better able to control informational narratives and conduct their warfare in such a way that it prevents the target state from unleashing all of its 'hard' and 'soft' power to defeat it. The social space has always been a necessary core to any uprising or rebellion, and serves as an incubator for ideology and political aspirations. The internet age provides an advantage to non-state actors that participate in the grey zone, because of the asymmetric informational advantage for collection and dissemination of information. The spread of the internet, social media apps, and portable electronic devices, adds to the uncertainty in the globalized world where no single state can exert control over the informational narratives in a conflict. An American airstrike may kill a terrorist in the foothills of Pakistan, but if local actors can shape the death narrative as unjust indiscriminate violence, then it undermines the outcome intended.

Hybrid Warfare

Hybrid warfare is a military strategy which employs political warfare blended with conventional warfare, irregular warfare and cyber warfare and other influencing methods, such as fake news, diplomacy and foreign electoral intervention. A state sponsor of a hybrid campaign must guard his movement without triggering a conventional kinetic response by the victim state and its allies. The center of gravity of a victim state is the ability of its security forces to handle the separatist insurrection. The United States used kinetic hybrid techniques to bring down regimes in Afghanistan and Libya. Nowadays, more states in the world are fighting non-state players than ever before. These enemies can be religious zealots (ISIS, Al Qaeda, Boko Haram), separatists (Pakistan sponsored groups in Kashmir, Kurdish groups, Ukrainian groups), revolutionaries (Naxalites) or just criminal gangs ((drug cartels). All these require grey zone strategies.

Grey Zone and Space Support

Space makes great contribution to grey zone conflict. Space based platforms are used for Intelligence, Surveillance and Reconnaissance (ISR), communications (telephones, internet, TV), navigation (GPS, Beidou), targeting, among others. Space operations have the advantage of ambiguity, because attribution may be difficult. Also the damage assessment can be difficult in space. Ambiguity is key to grey zone activities. Grey zone conflict in space requires policymakers understand and wield influence in space. Space doctrines the world over concentrate on space power and space control, but do not address space influence. Space deterrence is today beyond kinetic operations against space assets. It includes non-kinetic space operations such as jamming, dazzling (laser) or spoofing. Threatening enemy C4ISR in contingencies may affect their grey zone operations. In grey zone conflict the adversaries can conduct reversible space operations. There is a saying that ‘Uninhabited satellites have no mothers’. There is likely to be less moral and emotional response to destroying/affecting space resources.

Airpower - Significant Influence in the Grey Zone

Airpower is often used as in context of air-delivered firepower or the capability to project conventional forces anywhere in the world. But now, the air forces the world over are equipping and optimizing for low-intensity conflict scenarios. While their conventional footprint remains heavy, their existing special operations aviation capabilities offer a range of grey zone operations. Special operations fixed-wing and rotary-wing aircraft, unmanned aerial vehicles (UAV), ELINT and Electronic Warfare (EW) platforms, Synthetic Aperture Radar (SAR) and other ISR aircraft support grey zone operations. There is a need for recalibrating airpower for the grey zone operations by focusing on logistics and communications. Small civil aviation aircraft too have capabilities for grey zone requirements. It is less about tonnage but more about critical cargo that may be delivered at short distances. Civil drones with cameras, civil aircraft flown by civil pilots, to deliver individuals and cargo into highly isolated locations support grey zone ops.

Grey Zone Aerial Logistic Support

The ability to quickly move individuals and equipment into disputed areas without having to use, sometimes contested, surface means brings asymmetric advantage. Short roads or soccer fields allow landing and take-off by small aircraft. Vertical-lift drones allow operations even to urban areas. Automated quad copters can rapidly move critical supplies. Electric vertical takeoff and landing air taxis are already operating in some countries. Militaries are benefiting from some of these evolutions in civil aviation.

Small Team Insertion

In grey zone conflict, small teams or even single individuals are important. Russian operations in Ukraine found that the most valuable individual was the ‘agent in charge’ who infiltrates target area to develop intelligence networks and undermine local resistance. To move operatives, the ability to insert counter-intelligence teams – or to extract agents – is a legitimate application of grey zone airpower. Ability to deliver small payloads, particularly anti-tank or anti-aircraft teams, can have great impact in a low-level conflict. Rapidly moving small teams,

remote weapons, sensors, or critical supplies will be important where the detection or destruction of even a single tank can be the critical for long-term success.

Aerial Communications

Airpower greatly supports to enhance and reinforce civil communications capabilities in grey zone battlefields. It allows to maintain real-time communications, even without existing infrastructure. Civil airborne platform also provides an un-attributable asset. Small telecommunications chips can be used to build a reliable, self-healing, encrypted network, and airdropped. A single aircraft could make a low pass and drop hundreds of nodes over a wide area. These could be used for maintaining situational awareness, sustaining counter-propaganda efforts, or other purposes. Thus enabling cyber teams to exploit otherwise closed communications.

Intelligence Gathering

Positioning elevated aerial sensors is an important role of airpower. Actual interpretation of intelligence is the job of other agencies. UAV help obtain accurate timely information in conjunction with air-inserted communications network. Detect and attribute hostile actions and deprive them deniability. Airborne cell phone trackers could be used to intercept and track cell phone usage. It helps provide real-time intelligence, and also expose the participants by identifying and tracking proxies who rely on smart phones for command and control. Small air-launched drones such as the Perdix, meant for swarming applications, can help set up sensor relays for larger communications coverage. Many militaries the world over have begun banning smart phones and social media use for official purposes.

Air Expeditionary Task Force

The major air forces have Air Expeditionary Task Force launching capabilities, and global reach. They provide intra-theater mobility, and are part of the capability built for Airborne operations. Air Force's also have large helicopters fleets that can be escorted by attack helicopters and given fighter cover. Clearly short and vertical takeoff aircraft do help operate from semi-prepared or even damaged airstrips.

Small Team Support by Air

The military tactics of distributed combat operations using specialized troops operating in small, rapidly shifting groups would be very handy in grey zone operations too. These capabilities used for grey zone warfare also support regular operations in an anti-access/area denial environment. Aviation will support clusters of field locations with personnel, tools, equipment, and munitions. They could deliver or rapidly replenish ammunition, ready-to-eat meals and basic supplies to sustain a platoon sized force. Delivery drones could provide critical spare parts or repair kits. Like all aircraft, these platforms could be vulnerable to air defence systems, and forces them to fly at extremely low levels to avoid heat-seeking, shoulder-launched weapons. Propeller aircraft and electric motor powered aircraft would be safer from existing infrared seekers, but such aircraft will be vulnerable to anti-aircraft guns and small arms.

Big Power Grey Zone Ops

The United States initiated military, political, and proxy operations in Iran, Guatemala, Vietnam/Indochina, Chile, Angola, Afghanistan, Nicaragua, and Panama, among others. Most of these actions violated international laws, treaties, and norms, but the United States engaged in them anyways. The Soviet Union operated along similar lines in trying to subvert other countries toward Soviet interests in Eastern Europe, central and South America, and some non-aligned states in Asia. More recently ISIS fighters, Houthi Rebels, and Taliban insurgents managed significant territorial gains in the face of airstrikes. Syria and Iraq are cases of a quasi-state revolution formed out of a mix of terrorists, insurgents, criminals, warlords, ex Saddam troops, and religious zealots. ISIS leaders used political messaging to increase recruitment and win over militant groups.

Chinese Grey Zone Approach

China is trying to infiltrate poor countries through Belt and Road Initiative (BRI) and using debt diplomacy by giving cheaper, sometimes unreturnable, loans. China has supplemented these strategies with growing employment of economic coercion and political subversion.

China is also using cheap exports, and embedding the electronic systems with snooping devices. It is making efforts to impregnate Tibetan and Xinjiang population with its own beliefs. It is making efforts to change the status quo of territorial sovereignty and administrative control of the Senkaku Islands through grey zone tactics. Chinese successfully used grey zone aggression in the South China Sea. These tactics include China's unprecedented expansion of artificial islands, as well as the use of law enforcement and maritime militia vessels. China is also using state backed media and social media Apps to peddle influence and ideology.

Most importantly, China is making huge investments in aerospace, one of the key areas that will one day support its grey zone operations. China's preferred approach is to deploy air assets in strategically important waterways that are sensitive to others without breaching territorial airspace. Y-8 airborne early warning aircraft and H-6 bombers of the PLA Air Force have been flying through the Miyako Strait (between Miyako and Okinawa Islands). In November 2013 China declared an air defence identification zone (ADIZ) in the East China Sea, and applying the foreign aircraft rules that are beyond the scope of traditional ADIZ practices.

Grey Zone Regulation

Activities in the grey zone such as intelligence or information operations are difficult to regulate. The relationship between governments, technology and media companies, and the way in which their services are used for propaganda or subversion, are complex and need scrutiny. Counter-terrorism and counter-radicalization are areas of world attention. Normally, existing conventions and regulations should be extended into the activities in the grey zone. That will once again require sustained multilateral effort. The world cannot sit back and accept that the grey zone is a place where rules do not apply. Bad behavior cannot be encouraged and may raise the risk of miscalculation and escalation.

Grey Zone Threat India

India has been facing a hybrid grey-zone threat, including criminal aggression, for long. The increased radicalization in the neighbourhood has opened up new grey-spaces and caused tension

between state and non-state actors in whole of South Asia. Violent extremist organizations such as the Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM) are leveraging tacit support from Pakistan government to carry out irregular warfare. Infiltration of sleeper cells from Myanmar and Bangladesh to launch grey zone ops in India is of concern. Grey zone provocations are meant to neutralize India's conventional strength vis-a-vis Pakistan, and encircle and keep India embroiled by China. Many insurgent groups in India are backed and funded by China and, for long, China has been actively deploying the media for psychological warfare to weaken India. The Chinese Communist party's media mouthpiece Global Times write-ups regularly try shape international opinion including anti-India sentiments. China also sends subtle warnings to dissuade India from political and military activity in Arunachal Pradesh; it claims to be its own. China's has recently installed marine observatories in the Exclusive Economic Zones (EEZ) of Pakistan and Maldives, for naval surveillance in the garb of marine scientific research. China is also engineering 'net-wars' launched by so called anonymous non-state actors who are well trained Chinese professionals. India has to contend with low-intensity sporadic attacks launched against security forces in Kashmir, Naxal areas and North east.

Indian Air assets for Grey Zone Ops

Indian special operations forces would need near real-time intelligence. India's advances in space-based surveillance, induction of a large number of aerial surveillance platforms including Airborne Early Warning and Control System (AEW&C), aircraft with SAR and ELINT sensors, UAVs and aerostats give it better capability. Radio, radar, and even satellite communications systems are in place. Night-observation cameras, long-range detection radars, motion sensors, and thermal imaging systems. IAF already operates three PHALCON airborne warning and control systems (AWACS) and two more are on order. IAF also has two 'NETRA' AEW&CS. Many IAF fighter aircraft carry Recce pods. IAF's secure AFNET and IACCS allow net-centric operations. The C-130 J Hercules is a special operations aircraft. IAF has significant airlift capability for airborne operations. The Chinook and Apache give

it significant additional heliborne special ops capability. But surely a lot more needs to be done to tackle two complicit neighbours.

Grey Zone Air Operation - India

Balakot air strikes against the JeM terrorist training camp in the Khyber Pakhtunwa province of Pakistan was India's employment of offensive air power in sub-conventional operations and can be termed as a grey zone operation. Indian political quest for restraint in the application of force and especially reluctance to use air power in pursuing counter-insurgency, counter-terrorism and counter-infiltration operations due fear of escalation finally was broken. IAF has maintained doctrinal clarity on sub-conventional air operations. The political executive finally showed the Will. Interestingly in its formative years in 1930s, IAF Audaxes and Wapitis, were used to strafe and bomb insurgents in Waziristan. A heliborne operation supported by offensive air power was used against Mizo National Front (MNF) and also Nagas in 1960s. Air power was used in the operations by Indian Peace Keeping Force (IPKF) in Sri Lanka. IAF air operations against Naxal insurgents include ISR and casualty evacuation.

Options India

Each case of grey zone activity is likely to be unique, so the correct set of responses to a given action will depend on the circumstances at the time. There is an ongoing grey zone aggressive competition among USA, Russian and China. What would one do to a Chinese swarming attack, or accelerated cyber and disinformation attacks? Overarching strategic concept for responding to grey zone threats would be to try build and shape an international context supportive of India. Pakistan is also using grey zone tactics on the ground by infiltrating and training cells in India. Large bureaucratic states that are slow to adapt and counteract such forces lose out. India must prepare to deter China and Pakistan from extreme forms of grey zone aggression. The ability of Indian special operations forces to conduct low-visibility, irregular warfare operations need to be strengthened and exploited. Significant funding is needed for this purpose. Need to caution and dissuade Indian population about the grey zone techniques and build and sustain resilience. Build new

military capabilities in key locations, anticipating political meddling and blunting the effects with information operations planned in advance. An important part of any grey zone response strategy is to undertake institutional reform, including setting up a core organization at national level with a selected staff, to run counter grey zone campaigns.

The attack at Mumbai on 26/11 of 2008 showed glaring shortcomings in civil-military integration which is an imperative in grey zone conflict. There is need for better integration of non-kinetic capabilities among armed forces. It is advisable for India to graduate from simple deterrence to a more proactive stance where mutual violence and mutual hurt are leveraged to secure favourable outcomes. While applying 'top-down' solutions, there is also a need to address emerging threats and conflicts from the 'bottom-up' by considering the local politics that may drive warfare at the national level. IAF and Indian Army need to train jointly for the counter-terrorist operations. Early operationalisation of the Chinook and Apache helicopters will enhance capability. India needs to get its act right. India has also to take advantage of air power as a major force multiplier in the grey zone operations.

***Air Mshl Anil Chopra, PVSM, AVSM, VM, VSM (Retd)** is a well known Delhi based defence analyst and author.

GREY ZONE ACTIVITY IN MARITIME ASIA

Vice Adm HCS Bisht, PVSM, AVSM, NM (Retd)*

Introduction

Today's geopolitical conflicts indicate a trend by some countries to gradually, but fundamentally revise the regional or global system of alliances and international norms to suit their national interests. This process of conflict-induced change comes in the category of grey-zone conflict, in which states conduct operations that only occasionally pass the threshold of war. Grey-zone operations generally refer to those conflicts – at times not violent –and frequently characterized by an ambiguous point of victory[1]. Another definition of 'Grey Zone' Operations is that it 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.[2] 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. As per US RAND Corporation analyst Michael Mazarr, 'Grey zone' strategies have three primary characteristics. They seek to alter the status quo. They do so gradually. And they employ "unconventional" elements of state power.[3]

It is also important to distinguish between the strategic goals of grey-zone conflict and the tactical operations of hybrid warfare. The

1 Canadian Global Affairs Institute, Policy Paper, War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare, by David Carment, CGAI Fellow and Dani Belo, October 2018

2 Deciphering Grey Zone Operations in Maritime Asia, Abhijit Singh

3 Dmitry Filipoff, "Andrew S. Erickson and Ryan D. Martinson Discuss China's Maritime Grey Zone Operations," Center for International Maritime Security (CIMSEC), 11 March 2019. Republished as "Interview: China's Maritime 'Grey Zone' Operations," The Maritime Executive, 2019

two are not synonymous. Unlike hybrid warfare, grey-zone conflict participants rely on unconventional tactics that do not cross the threshold of formalized state-level aggression. In other words, hybrid warfare can be a tactical subset of grey-zone conflict deployed under certain conditions and in varying degrees. [4] In making this distinction, we are better positioned to understand the spectrum of states that are engaged in grey-zone conflict while drawing on different kinds of grey zone operations/hybrid tactics.

Whilst discussing Grey zone and hybrid operations, there is no clearer example than Asia since it has always been considered the hotbed of conflict and less than war operations, be it on land or in the maritime domain, by virtue of various factors like large population, a no of hotspots based on religion, ethnicity, resource inequality, scourge of terrorism etc. Some examples of these operations being carried out in various regions of Asia in the maritime domain are elucidated in the succeeding paragraphs.

Grey Zone Operations by China

As China was propagating its peaceful rise in the 80s and 90s, with a veil shrouded in secrecy around its military modernization, its political, economic and military tacticians understood that to successfully promote the country's interests globally, direct military engagement vis-à-vis the U.S and its allies would not be an option. Moreover, any direct confrontation could trigger a nuclear response, which would yield no positive outcomes for any of the parties. Activities targeting weaker opponents are largely meant to undermine the strength and unity of alliance structures surrounding other powerful states. Thus, even though the development of a conventional force remains a priority for China, the country would largely forgo its use in favour of unconventional tactics, that would remain between the thresholds of open war and peace. In 1999, two Chinese military (PLA) officers reflected on this in '*Unrestricted Warfare'*, in which they advance the concept of combining unconventional and covert tactics against the U.S. [5]

4 War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare, by David Carment, CGAI Fellow and Dani Belo
October 2018

5 Unrestricted Warfare, Qiao Liang and Wang Xiangsui, Feb 1999

As per inputs available, the PLA has generally identified four alternatives to traditional military engagement: (a) Political action to promote favourable global change in policy and international norms (b) Increasing economic pressure on allies and opponents by its so called 'Cheque Book diplomacy', wherein China is able to promote its interests on a global scale and even change partnership priorities of individual countries (c) Use of cyber warfare and (d) Incorporation of non-state actors into conflicts. Over the past decade, China's actions largely adhered to these principles. Some examples of such actions by China are cyber-attacks against 34 U.S. companies, including military contractors and another instance was the breach of Australia's Security Intelligence Organization by China in Jan 2013.[6]

China's island-building spree in the Parcels and Spratly Islands and the facilities constructed on them is unprecedented in size and scope. These features now allow China to maintain a large military air and naval presence over the entire South China Sea under the guise of civilian purposes, such as protection of the global commons, Search and Rescue and Science observation. Since 2014, China has reclaimed over 3200 acres of land on seven disputed features in the Spratlys, and 50 acres of land in the disputed features in the Paracels.[7] China has constructed the full array of dual use facilities on these features, to include large airstrips, harbours, aircraft hangars, barracks, large communications sensors and radar arrays, hardened shelters for missile platforms and large underground tunnels for ammunition, water and fuel storage. By overwhelming all over claimants in terms of size of reclaimed land and military facilities in the South China Sea, China now has the capability to monitor and exert peacetime military coercion over civilian and military air and surface activities in these disputed waters.

China has very successfully used the 'String of Pearls' policy in the last decade to not only engage with the African nations but she has also significantly challenged the traditional U.S influence in the

6 Canadian Global Affairs Institute, War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare, BY David Carment, CGAI Flellow and Dani Belo, Oct 18

7 Maritime Issues-Rand Corporation Grey Zone Challenges in the East and South China Sea By Lyle J. Morris January 7, 2019

region. For example, a historic meeting between Chinese leaders and representatives of 48 governments in Africa took place in Beijing in November 2006, while the U.S. was preoccupied with the war in Iraq. This meeting paved the way for future investments in traditional U.S. allied states such as Angola and Nigeria, where China initiated long-term infrastructure and communications projects. This trend has created economies entirely dependent on Chinese investment.

Means employed to undertake Grey Zone Ops by China in the Maritime Arena

China Coast Guard (CCG)

An important vehicle used by China in enforcing its 'Grey Zone' Operations in the Maritime domain is by the use of the Chinese Coast Guard (CCG) and the People's Armed Forces Military Militia (PAFMM). The CCG is responsible for a wide range of missions under the umbrella of maritime rights protection, including enforcement of China's sovereignty claims, surveillance, protection of fisheries' resources, anti-smuggling, and general law enforcement. As of July 2018, the CCG completed its merger into the military command structure through its subordination to the PAP, which could facilitate closer coordination between the CCG and the PLA Navy (PLAN). China primarily uses paramilitary maritime law enforcement agencies in maritime disputes, selectively using the PLAN to provide overwatch in case of escalation. Recently, a few days after the administrative transfer of the CCG to the People's Armed Police (PAP), the CCG conducted a patrol mission near the contested Senkaku Islands in the East China Sea.

The CCG's rapid expansion and modernization has improved China's ability to enforce its maritime claims. Since 2010, the CCG's fleet of large patrol ships (more than 1,000 tons) has more than doubled from approximately 60 to more than 130 ships, making it by far the largest Coast Guard force in the world and increasing its capacity to conduct simultaneous, extended offshore operations in multiple disputed areas. Furthermore, the newer ships are substantially larger and more capable than the older ships, and the majority are equipped with helicopter facilities, high capacity water cannons and guns ranging from 30 mm to 76 mm. A number of these ships are capable of long-endurance out-of-

area operations. These characteristics give CCG vessels the ability to intimidate local, non- Chinese fishing boats, as occurred in an October 2016 incident near Scarborough Reef.

In addition, the CCG operates more than 70 fast patrol combatants (more than 500 tons), which can be used for limited offshore operations as also more than 400 coastal patrol craft and approximately 1,000 inshore and riverine patrol boats. The CCG is likely to add another 25-30 patrol ships and patrol combatants by the end of the decade before the construction program levels off.[8]

People's Armed Forces Maritime Militia (PAFMM)

The PAFMM is a subset of China's national militia, an armed reserve force of civilians available for mobilization. Militia units organize around towns, villages, urban sub-districts and enterprises and vary widely in composition and mission. In the South China Sea, the PAFMM plays a major role in coercive activities to achieve China's political goals without fighting, part of the broader Chinese military theory that sees confrontational operations, short of war as an effective means of accomplishing political objectives. The militia has played significant roles in a number of military campaigns and coercive incidents over the years, including the 2009 harassment of the US vessel *USNS Impeccable* conducting normal operations, the 2012 Scarborough Shoal standoff, the 2014 Haiyang Shiyou-981 oil rig standoff and a large incursion in waters near the Senkakus in 2016.

A large number of PAFMM vessels train with and assist the PLAN and CCG in tasks such as safeguarding maritime claims, surveillance and reconnaissance, fisheries protection, logistic support and Search and Rescue. The government subsidizes various local and provincial commercial organizations to operate militia vessels to perform "official" missions on an ad hoc basis outside of their regular civilian commercial activities. In the past, the PAFMM rented fishing vessels from companies or individual fishermen but China has built a state-owned fishing fleet for at least part of its maritime militia force in the South China Sea. The Hainan provincial government, adjacent to the South China Sea, ordered

8 US Department of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2019, p 52

the building of 84 large militia fishing vessels with reinforced hulls and ammunition storage, which the militia received by the end of 2016, along with extensive subsidies to encourage frequent operations in the Spratly Islands. This particular PAFMM unit is also China's most professional. Its forces are paid salaries independent of any clear commercial fishing responsibilities and recruited from recently separated veterans.[9] The maritime militia allows China to harass foreign fishermen and defy other Coast Guards operating in the near seas substantially, without obviously implicating the Chinese state. Given its employment history and the high level support that it receives, it seems clear that the maritime militia is seen as a key element in Beijing's overall vision of becoming a maritime power, at least when it comes to co-operation with the CCG and PLA Navy in protecting its maritime interests in China's near seas.

Over the past few years, as China has continued its expansion in the maritime domain, scholars and practitioners alike have honed in on the subject of how Beijing operates in the so-called "grey zone" between war and peace, staying below the threshold of armed conflict to secure gains while not provoking military responses by others, including the United States. Understanding the dynamics of this has important implications not only for particular maritime spaces, such as the East China Sea and the South China Sea, but also for broader issues such as the management of U.S.-China competition and wider regional peace and stability.

Chinese policymakers are very clear about the fact that their long-term goal is to exercise "administrative control" over all of the 3 million square kilometers of Chinese-claimed maritime space. This includes all of the Bohai Gulf, large sections of the Yellow Sea and East China Sea and all of the area within the nine-dash line in the South China Sea. Many Western analysts assume that China has more abstract aims, like discrediting the international legal order. This may happen anyway, as a byproduct of their actions, but the most compelling evidence suggests that Beijing sees strategic, economic, and symbolic value in controlling as much space as possible within the First Island Chain.

9 US Department of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2019, p 54

Chinese leaders don't use the term "grey zone" to describe their approach to asserting control over this space. For at least a decade, they have conceived of their policy as a balancing act. On the one hand, they feel the need to defend and advance China's claims. They call these actions "maritime rights protection." On the other hand, they want to avoid severely harming their relations with other states. Regional stability, after all, is vital for sustaining China's economic development — which remains the core of China's grand strategy. Using paranaval forces like the CCG and the PAFMM allows them to find an optimal balance between "rights protection" and "stability maintenance." Paranaval forces are much less provocative than grey-hulled warships. The Chinese coast guard operates on the pretext of routine law enforcement, and militia often pretend to be fishermen. Yet both forces can be used to pursue traditional military objectives of controlling space.

The CCG and the PAFMM perform the vast majority of Chinese maritime grey zone operations. Chinese strategists and spokespeople frame their actions as righteous efforts to protect China's "maritime rights and interests." The CCG uses law enforcement as a pretext for activities to assert Beijing's prerogatives in disputed maritime space. PAFMM personnel are often disguised as civilian mariners, especially fishermen. Most do fish, at least some of the time. But they can be activated to conduct rights protection operations. And a new elite subcomponent is paid handsomely to engage in sovereignty promotion missions fulltime without fishing at all. Meanwhile, the PLA Navy also plays a role in disputed waters, serving what Chinese strategists call a "backstop" function. It discourages foreign countries from pushing back too forcefully and stands ready over the horizon to come to the aid of China's grey zone forces should the situation escalate.

Grey-Zone Operations in South Asia

Grey Zone activities are an international phenomenon and there has been some debate over such operations in South Asia also from non-state actors in the littoral seas. Our western neighbour, Pakistan known internationally for its support for terrorism, can not be far behind in instances of Grey Zone activities and this can best be understood by recounting some experiences of the Pakistan Navy and their infamous experience with terrorists.

In August 2014, the Al Qaeda carried out an attack on Pakistan's Naval Dockyard at Karachi, with an aim to hijack PNS Zulfikar, a Pakistan Navy frigate. The ship at that time, was preparing to sail for an international Naval exercise. Some Al Qaeda militants, approached the ship in an inflatable boat wearing Naval uniforms. They apparently had information about the loose security arrangements on the ship and as they closed the ship, a lone sentry onboard observed their suspicious movements and alerted senior security personnel. A gunfight ensued and fortunately for the PN, the attackers were subverted. It later came to the fore that among those who helped Al Qaeda carry out the attack were radicalized cadres of the Pakistan Navy. On deeper analysis of this incident, it is no surprise that the attackers in connivance with PN knew all about sailing and operating the warship, otherwise they wouldn't have attempted an operation as complex as this. According to an initial statement from al Qaeda, the plan was to use the Zulfiqar to attack a U.S. navy vessel, meaning potential loss of American lives and a blow to relations between the two nations. A further statement issued by the group identified the target as USS Supply, a US naval ship used to refuel warships at sea. As per the statement, the Indian navy was also a target.[10]

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. The attack had followed failed talks between the Pakistan Navy and Al Qaeda over arrested navy personnel with suspected links to the militant organization. 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. [11]

10 REUTERS, In attack by al Qaeda, lines blur between Pakistan's military, militants Syed Raza Hassan, Katharine Houreld, October 1, 2014

11 Deciphering grey-zone operations in maritime-Asia- ORF Policy Paper by Abhijit Singh

Arguably, the most conspicuous manifestation of the grey zone phenomenon in South Asia came in the form of the 26/11 terrorist attacks on Mumbai, which were masterminded in Pakistan and shook the Indian security establishment. In November 2008, ten heavily armed Pakistani Lashkar-e-Taiba (LeT) terrorists, supported by Pakistan Navy and Pakistani intelligence agencies hijacked an Indian fishing boat 'Kuber' off Gujarat coast and disembarked off Nariman Point/Cuffe Parade area in Mumbai with arms and ammunition. They created mayhem by taking control of two premier hotels in Mumbai, killing 166 people and injuring over 300 in South Mumbai.

Grey Zone Operations in West Asia in 2019

Another glaring example of 'Grey Zone Operations' carried out recently was in West Asia in mid 2019. It stemmed from the escalation of military tensions between Iran and the US, following the deployment of military assets to the Middle East, due to intelligence suggesting a planned campaign by Iran and allies against US forces and interests in the region. Following Iran's shooting down of a U.S. Navy surveillance drone on 20 June 2019, the U.S. bolstered its efforts to establish a coalition to deter Iranian attacks in the Persian Gulf. On 19 July, the US launched 'Operation Sentinel' with the stated goal of de-escalating tensions and promoting maritime stability in international waters "throughout the region". It also called for providing escorts to their flagged commercial vessels in the region and for coordinating surveillance capabilities. Japan and India sent their own separate Naval assets to the region to escort their respective merchant vessels.

On 12 May 19, four commercial ships, including two Saudi Aramco oil tankers, were damaged near the UAE port of Fujairah in the Gulf of Oman. The UAE stated that the incident was a "sabotage attack", while a US assessment reportedly blamed Iran or Iranian "proxy" elements for the attack. Tensions reached a new high when, on 20 June, Iran shot down a U.S. Navy RQ A-Global Hawk surveillance drone, saying that the drone violated Iranian territorial waters and airspace. Iran and the United States provided conflicting GPS coordinates for the drone's location, making it unclear whether the drone was within Iran's territorial waters. On June 22, it was reported that in another example of 'Grey

Zone operations' President Trump had approved cyber attacks that disabled Iranian Revolutionary Guards computer systems used to control rocket and missile launches on the night of the drone-downing. The cyber strikes were handled by US Cyber Command, in conjunction with U.S. Central Command. [12]

On July 18, according to the Pentagon, USS Boxer which was patrolling the area, took defensive action against an Iranian drone that had closed the ship in the Persian Gulf to approximately 1,000 yards and jammed the drone, causing it to crash at sea. Earlier, on July 14, a Panamanian-flagged oil tanker, MT Riah, which was operating in the United Arab Emirates, disappeared from ship tracking maps near Iran after crossing the Strait of Hormuz. Adding to the mystery, no entity claimed ownership of the tanker. On July 20, the British-flagged tanker 'Stena Impero' was seized in a raid by Iranian Revolutionary Guard forces and its crew of 23 detained on board. On September 4, Iran decided to free only seven crew members of the detained British tanker. A second British-owned and Liberian-flagged ship was also seized but later allowed to continue its journey. In a letter to the UN, Iran stated that the 'Stena Empero' had collided with and damaged an Iranian vessel, and ignored warnings by Iranian authorities.

Iran confirmed that it seized the ship as retaliation over the British seizure of 'Grace 1' in Gibraltar and hinted that it would be willing to release 'Stena Empero' in exchange for the release of 'Grace 1'. On August 4, 2019 the Iranian Revolutionary Guards seized an Iraqi tanker for allegedly smuggling oil to other Arab Countries. The 7 crew members on board were detained further heightening tensions in the Persian Gulf. It was just days later that Britain and Israel joined the Sentinel Program to protect oil tankers in the Persian Gulf. On September 16, 2019,Iran seized another vessel near the Iran's Greater Tunb island in the Persian Gulf but was later released. Another glaring example of Grey Zone Operations is the 'Gulf of Aden' patrol by ships of various Navies to escort their merchant shipping. This operation has been going on since 2008, wherein a large no of Navies are involved in operations against Somali piracy where despite a large international naval presence acts of piracy are still reported.

12 www.wikipedia.org/Persian Gulf 2019

Conclusion

As the Prussian theorist of war, Carl von Clausewitz argued, war is an ever-evolving, interactive phenomena. Understanding the complexity and distinctions of various modes of warfare conducted across the continuum of conflict is critical, as is understanding our adversaries, their methods, and conceptions of victory. The maritime domain provides the right mix of anonymity and secrecy for conduct of Grey Zone operations should the need be. Also the Indian Ocean Region (IOR) is the hub centre of maritime activity, where all major powers are jostling for space, since more than half the world's trade passes through the multitude of Sea Lines Of Communications (SLOCS) straddling the Indian peninsula. All major maritime powers have their eyes fixed on the IOR and deploy their naval platforms on a regular basis in order to protect their maritime interests. The PLA Navy has particularly been taking keen interest in the region and regularly sending their Naval ships and submarines to literally 'test waters' should the need arise. Since Sep 2014, the PLA Navy has sent numerous ships and submarines to the region, at times on the ruse of combating piracy in the Gulf of Aden, in order to study the hydrology around our waters so as to determine areas for deployment of their submarines during a possible conflict. They had sent both nuclear and conventional submarines along with an escort ship each, with the aim of doing a test run, which also included berthing arrangements at Colombo port in Sri Lanka and Gwadar port in Pakistan. After India made noise during President Sirisena regime in Sri Lanka, the submarine visits apparently came down. However, given that the new political leadership in Sri Lanka is better disposed towards China, we may see increased frequency of PLA Navy ships and submarines operating in our waters since they can stop over at Colombo/Hambantota and undertake operational deployments from there, after logistics replenishment as required. This is another category of 'Grey Zone' operations which the Chinese are adept at.

***Vice Adm HCS Bisht, PVSM, AVSM, NM (Retd)** Is a former Director General Indian Coast Guard and Flag Officer Commanding in Chief Eastern Naval Command.

HYBRID WARFARE TO WARFARE IN GREY ZONE: A SMART TRANSITION

Brig (Dr.) Rajeev Kumar Bhutani (Retd)*

Introduction

Warfare is "the mechanism, method, or modality of armed conflict against the enemy".[1] While war has not changed for thousands of years, warfare, specifically the technique or tactics and technology used to conduct war, has been constantly changing.Traditionally, warfare is classified in to two categories – conventional and irregular. Each served a fundamentally different strategic purpose that determinedvaried approaches to its conduct.[2] Hybrid threats bridge the gap and combine aspects of these two types of warfare in a single space and time.

Hybrid warfare or hybrid threats are not new. Hybrid threats have been used as the alternative solution for conventional military conflicts since many years. Arguably, American colonists used hybrid tactics against the British in the Revolutionary war. The first truly modern hybrid war was the Soviet – Afghan conflict of 1979-80. Although, the anti-Soviet non-state Mujahedeen did most of the fighting against the Red Army and its Afghan puppet government, the United States provided the modern arms and technical advisors that kept the insurgents in the field. The Americans were careful to avoid direct conflict with the Soviet forces.[3]

However, after the end of Cold War, it was the 2006 Israel – Lebanon War, where Hezbollah (backed by Iran) employed a host of different tactics against Israel, which included guerilla warfare, innovative use of technology and effective information campaigning. Following that war, the term 'hybrid warfare', as currently used, was first introduced by U.S. Marine Corps Lieutenant Colonel Frank G. Hoffman in 2006;[4] though Hoffman stated that he took the term from a thesis by Robert G. Walker in which Walker described conduct of low intensity operations

by the US Marines. In 2006, Hoffman referred to the phenomenon as "complex irregular warfare", building further on work he conducted with US Marine Corps General James Mattis (later US defense secretary) in 2005 in an opinion piece in United States Naval Institute Proceedings Magazine.[5]In 2007, Hoffman gave the first definition of hybrid warfare. According to him, "Hybrid wars can be conducted by both states and a variety of non-state actors. Hybrid Wars incorporate a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."[6]The July 2006 war between Israel and Hezbollah is generally considered as the textbook example of hybrid warfare.

Subsequently, Russia's annexation of Crimea in 2014 and undeclared war in Eastern Ukraine – as Russian covert operatives and military units played crucial roles in both – have brought this subject to the forefront of discussion amongst the security analysts and academia. The Russian military and hybrid activities have only reinforced the impression that hybrid war is the new Russian way of war and even a major driver of Russian foreign policy.[7]On the heels of Russia's actions in Eastern Ukraine, China also carried out expansion in the South China Sea. The defense and academic communities have come up to describe these conflicts in the 'Grey-Zone'. The grey-zone is an operational environment or the "space" between peace and war on the spectrum of conflict. According to defense and foreign policy analyst Dr. Nadia Schadlow, "the space between war and peace is not an empty one – but a landscape churning with political, economic, and security competitions that require constant attention".[8]

To analyze whether conflicts or warfare in 'Grey-Zone' is a continuum of 'Hybrid Warfare' or both are separate concepts, it is essential to study the following:

- Strategies and tactics adopted by Hezbollah during the Second Lebanon War in 2006;
- The Russian concept of 'Non-Linear Warfare' employed in Crimea and Ukraine;
- China's concept of Unrestricted Warfare; and

- Thereafter derive a linkage between Hybrid Warfare, Hybrid Threat and Grey-Zone.

The Second Lebanon War - 2006

As it is evident from the emerging trends, future conflicts will be multi-variant or multi-modal, where there will be blending or blurring of lines between modes of war. The greatest challenge in the future will not come from a state that selects a defined approach but from states or groups that select from a wide variety of tactics and technologies and blend them in innovative ways to meet their strategic objectives. This is especially true as hybrid wars can be conducted by both states and a variety of non-state actors.[9]

In the Second Lebanon War in 2006, Hezbollah clearly demonstrated the ability of non-state actors to conduct hybrid warfare. In the field, Israeli troops grudgingly admitted that the Hezbollah defenders were tenacious and skilled as they had proven more resilient and better-equipped than Israeli military forces anticipated.[10] The important aspects of this 34-day battle are: -

- Hezbollah's highly disciplined and well-trained distributed cells contested ground against a modern conventional Israeli Defense Forces (IDF), using a combination of guerilla tactics and technology in densely populated urban centers. Hezbollah skillfully exploited the narrow village streets as also built up areas to launch ambushes and evade detection and held strong defensive fortifications in close proximity to non-combatants.[11]

- The standard of training, fire discipline and lethal technology demonstrated by Hezbollah were much higher.

- Tactical innovations and novel application of technology by the defenders were noteworthy. In particular, the anti-tank guided missile systems employed by Hezbollah against IDF armor and defensive positions, combined with decentralized control, were a surprise. In the battle of Wadi al Saluki, a column of Israeli tanks was stopped in its tracks with telling precision. A total of 24 Israeli first line Merkava IV tanks of Brigade 401

entered the area, out of which 11 were destroyed by Anti-tank guided missiles.[12] This is the best example of blurring of conventional systems with irregular forces and non-traditional tactics.

- Hezbollah even managed to launch a few armed unmanned aerial vehicles (UAVs) (possibly three ababil drones) which required the IDF to adapt in order to detect them. A cause of concern for Israeli strategists was their global positioning system (GPS)-based navigation system, 450 km range and 40-50 kg explosive carrying capacity.[13]

- There is evidence that Hezbollah invested in signals intelligence and monitored IDF cell phone calls for some time and reportedly managed to decrypt IDF radio traffic. Hezbollah also seemed to have advanced surveillance system and very advanced night vision equipment.[14]

- Hezbollah's successful employment of "Noor" (C-802) Chinese-designed and Iranian-supplied anti-ship cruise missile to strike an Israeli naval vessel[15] represented another example of what 'hybrid warfare' might look like.

- Hezbollah's unique capability was its inventory of 12,000 to 13,000 rockets and ground-to-ground missiles, supplied to them by Iran and Syria. They were used both to terrorize the civil population and to attack Israeli military infrastructure. They managed to fire over 4000 rockets in to Israel between 12 July and 13 August. In spite of having short range and inaccuracy, they achieved strategic effects both in the physical domain by forcing Israel to evacuate tens of thousands of its citizens, and in the media by demonstrating their ability to lash back at the region's most potent military.[16]

Hezbollah's combat cells were a hybrid of guerillas and regular troops – a trend, which is likely to be emulated in future by others. In future, hybrid threats are likely to prove effective against large, modern and hierarchical organizations that are mentally or doctrinally rigid.

The Russian Concept of 'Non-Linear Warfare' Employed in Crimea and Ukraine

The Russian concepts have largely developed in response to U.S.-led military interventions in Kosovo / Serbia (1999), Afghanistan (2001) and Iraq (2003). On 26 February 2013, Chief of the Russian General Staff General Valery Gerasimov published an article *"The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations"* in Voyenno-Promyshlennyy Kurier (VPK) (Military-Industrial Courier). In this article, Gerasimov laid out his perspective of the recent past, present and expected future of warfare. This article was published about a year before the Maidan protests that set in motion the events leading to the eventual annexation of Crimea and Russian-sponsored insurrection in Eastern Ukraine. The chain of events that followed the Maidan protests could not have been foreseen by Gerasimov but his article is often cited in the West as 'Gerasimov Doctrine'.[17] In fact, Professor Mark Galeotti, Russian expert, published its translation in his blog with his own comments and claims to have coined the term 'Gerasimov Doctrine' to make his blog more attractive for people to read.[18]

There is a general consensus in Russian military circles that hybrid war is a completely Western concept as no Russian military officer or strategist has discussed it, except to mention the West's use of the term, or to mention the West's use of hybrid warfare against Russia.[19]

Gerasimov named the war of the future as "the war of a new generation" or the "Non-linear" warfare[20] and outlined its concepts as:

> "And the "rules of war" themselves have changed significantly. The role of non-military methods in achieving political and strategic goals, which in some cases significantly exceeded the strength of weapons in their effectiveness, has grown. The emphasis of the used methods of confrontation is shifting towards the widespread use of political, economic, informational, humanitarian, and other non-military measures – implemented with the use of the protest potential of the population. All this is complemented by covert military measures, including the implementation of information warfare and the actions of special operations forces. The open use

of force is often disguised as peace keeping and crisis settlement only at some stage, mainly to achieve ultimate success in the conflict."[21]

Some analysts consider 'Gerasimov Doctrine' as equivalent of the American Framework on the Adaptive Approach for the Use of Military Force (AAUMF), as the doctrine emphasizes the necessity of using military and non-military means against opponents.[22]

Gerasimov talked about something very different than the Western concept of hybrid war. One of the most interesting aspects of Gerasimov's article is the graphic illustration of relationship on the use of non-military and military measures in war, which showed that war is now conducted by a roughly 4:1 ratio of non-military and military measures. These non-military measures include economic sanctions, disruption of diplomatic ties, and political and diplomatic pressure. The salient difference is that the West considers these non-military measures as way of avoiding war while Russia considers these measures for war fighting.[23]

In Gerasimov's own words "Indeed, each war is a special case, requiring an understanding of its special logic, its uniqueness".[24] He meant that there was no set model or formula for understanding the operational environment or the exercise of national power in every war scenario. Each instance of a problem would be looked upon as a unique situation that necessitated the marshaling of the state's resources in whatever way is deemed fit.[25]True to the above philosophy, Russia employed different techniques in the Eastern Ukraine, Crimea and Baltics:

- In Eastern Ukraine, Russia relied on economic tools and cyber-space to harm its adversary's energy sector and infrastructure as well as non-state actors to fight against Ukraine's conventional forces. In 2014, during the unrest in Eastern Ukraine and the Maidan, the Russian government-operated Gazprom annulled the gas discount agreement, which the Yanukovych administration had signed. Further, in December 2015, Russia was accused of attacking Ukraine's power grid through cyber-space, thereby disabling a large

portion of the country's infrastructure. Russia aided the rebel forces of the LNR and DNR fighting against the Ukrainian Army.[26]

- In Crimea, working with the 16,000 uniformed forces already stationed (under a basing agreement with Kiev which permitted up to 25,000 soldiers to be stationed there), Russia deployed a covert military operation, using special unmarked military units to capture Ukrainian soldiers located at strategic government and military sites on the peninsula.[27]

- Since the Baltic States are members of the European Union (EU) and North Atlantic Treaty Organization (NATO), Russia employed unconventional tools to disrupt communications infrastructures as well as to provoke political unrest through appeal to the Russian diaspora. In October 2017, Russia launched a cyber-attack on Latvia, resulting in interruption of the country's emergency response telecommunications network.[28] Further, taking in to account the fact that Russian-speaking people make up about 30 percent of the population of Latvia and Estonia, Russia has been able to effectively use various information tools for promoting disquiet among the diaspora – highlighting the repressive and fragmented nature of minority rights in these countries.[29]

China's Concept of 'Unrestricted Warfare'

China has been increasingly involved in unconventional operations to dilute United States' hegemony. Though China avoids direct military engagement vis-à-vis the United States and its allies but its activities targeting weaker opponents are largely meant to undermine the strength and unity of alliance structures surrounding other powerful states. In spite of having its ambitions to develop a modernized conventional force on priority, China always prefers to use unconventional tactics that should remain between the thresholds of open war and peace.[30]

In 1999, two Chinese PLA officers, Colonels Qiao Liang and Wang Xiangsui brought out a book "Unrestricted Warfare" in which they advocated the concept of combining unconventional and covert tactics

against the United States. They generally identified four alternatives to conventional warfare: One, Political action to promote favorable global change in policy and international norms; Two, Increasing economic pressure on allies and opponents based on its burgeoning economy: Three, Engagement in cyber and network warfare; Four, Incorporation of non-state actors in to conflicts.[31] Over the past decade, China's actions have largely adhered to these principles.

Linkage Between 'Hybrid Warfare' and 'Warfare in Grey Zone'

Hybrid warfare is as old as the warfare itself. However, the modern concept of "Hybrid Warfare" takes its inspiration from Israel-Hezbollah War of 2006, after which U.S. Marine Corps Lieutenant Colonel Frank Hoffman took the initiative to define the Hybrid threats and introduced the term as it is being used in the present context. The Hezbollah's domination was so complete that the Winograd Commission, appointed by the Israeli government, concluded in its 2008 final report that IDF had failed to deter and defeat Hezbollah in South Lebanon.[32] Later on, relevance of Hybrid Warfare became more prominent in the context of antagonistic behavior between Russia and the United States.

Of late, Grey Zone or Grey Zone conflicts have entered in to the lexicon of Western security analysts and academics. The analysts have tried to split the post-2013 conflicts in to Hybrid Warfare and Grey Zone conflicts. To decide whether there is a linkage between Hybrid Warfare and Grey Zone conflicts or is there a smart transition from Hybrid Warfare to Grey Zone conflicts, one has to study and analyze the recent concepts propounded by various thinkers before arriving at a firm conclusion.

The senior officers of the U.S. Army Special Operations Command (USASOC) defined Grey Zone conflicts as a segment of the conflict continuum "characterized by intense political, economic, information, and military competition more fervent in nature than normal steady-state diplomacy yet short of conventional war."[33] While the hybrid threats are defined as "the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects."[34] Further, Grey Zone conflicts are those in which nation states and non-state actors use hybrid threats/tactics, such as fusing political

and information warfare with non-violent civil resistance, to achieve strategic objectives without violating international norms or crossing established thresholds and leading to open war.[35] For example, Russia used hybrid tactics to achieve its strategic objectives in destabilizing Ukraine and annexing Crimea without crossing a threshold that would draw other global powers in to the conflict against the Russians.

Thus, the Grey Zone encompasses the space between peace and war in which aggressors use hybrid threats to shape the battlefield and achieve strategic objectives short of all-out, declared conflict. It emerges that the Grey Zone is an operational environment and not a type of conflict or warfare, in the same way that Urban, Mountain or Desert Warfare are considered. Though, the tactics, techniques, procedures, and strategy used in each of these operational environment may differ, these areas or terrains do not qualify for a separate type of warfare in the same vein as Irregular or Conventional warfare. Similarly, Grey Zone describes conflict in an ambiguous operating environment in the "space" between peace and war.[36]

Differences Between Grey-Zone Conflict and Hybrid Warfare

Hybrid threats take place or are applied across the entire spectrum of conflict, whether it is Grey-Zone or open warfare. Hybrid threats employed are common to both. However, the major difference between the two are the overt use of conventional weapons / formations / tactics and a lack of ambiguity in open warfare hybrid threats, whereas the Grey-Zone hybrid threats are characterized by the use of special operations forces, irregular forces, and criminal networks employing a mix of conventional weapons and irregular tactics in a single space and time while striving for ambiguity and non-attribution.[37] A recent example is the Russians use of Grey-Zone hybrid threats in Eastern Ukraine, while in Crimea it used much more overt hybrid threats to annex the region. While not considered entirely a limited conventional war, Russia's actions to secure Crimea were overt enough to differentiate them from Grey-Zone hybrid threats, as Russia did not seek to hide its actions or to avoid violating international norms, such as annexing a part of another sovereign country that would entangle them in a broader conflict with Ukraine and upset the international community.[38]

In view of the aforesaid, following inferences can be drawn:

- Hybrid warfare does not exist as a separate form of warfare on par with irregular and conventional warfare. Hybrid threats or measures adopted are best described as tactics used throughout the modes of warfare to achieve the objective.
- While operating in the Grey-Zone, states often use proxies or work in concert with proxies, in order to maintain ambiguity that contributes to the confusion of actions in the Grey-Zone.
- Consequently, hybrid tactics and Grey-Zone conflict are not independent of each other; they are inextricably linked and aggressors use hybrid tactics across the spectrum of conflict to achieve the desired ends.[39]

Peculiarities of "Warfare in Grey-Zone"

Grey Zone is unique as the hybrid threats in it stay below the threshold of open conventional conflict between states, irrespective of whether there may be some shooting between states, state proxies and/or non-state actors. The main reason for this is that aggressors in the Grey Zone seek to take advantage of non-attribution to shape the battlefield to achieve their strategic objectives with minimal cost in terms of responses by other nations.[40] The key characteristics of 'Warfare in Grey Zone' are:-

- **Ambiguity.** In the Grey-Zone, ambiguity is essential to keep conflict in the space between peace and war. Aggressors always endeavor to maintain ambiguity through the use of proxies, such as criminal networks or militias, special operations forces, intelligence operatives, or through the use of civilians to achieve objectives through non-violent means. The aim of ambiguity is to maintain plausible deniability and thereby restrict the responses of international actors and institutions like the United States and the United Nations. In fact, Gerasimov Doctrine is also referred to as the Gerasimov Doctrine of Ambiguous Warfare, and was later transposed directly into Russia's 2014 Military Doctrine.[41] A recent example of an aggressor using ambiguity in the Grey-Zone was the Russia's employment of "unidentified troops" in Eastern

Ukraine. First, small groups of disciplined armed men without recognizable insignia captured local government buildings, including Ukrainian police stations and security service headquarters in towns across the Donbas. Then unarmed civilians quickly moved in, erecting barricades and surrounding the seized buildings, staging sit-ins and demonstrations in support of the rebels inside. In this way they became human shields for the armed men.[42] Most likely, these "unidentified troops" were Russian soldiers with out uniform but when they were present, the Ukrainians and rest of the world could not say with surety as to who was occupying the buildings prior to the arrival of civilians. The ambiguity played a key role in the Russians achieving their objectives in Eastern Ukraine with out attracting significant negative actions from international community.

- **Exploit Weaknesses of the Adversary Through Diplomatic, Information, Military and Economic (DIME) Instruments of Power.** Aggressors use a whole-of-government approach to exploit their adversary's weaknesses through the use of DIME instruments of power. Autocratic regimes like Russia can apply these more effectively because their leadership can focus on a single objective. In large democracies like the United States, bureaucracy is unable to synchronize efforts and information flow across various branches and departments. Hence, it often allows the aggressor to achieve its objective while the adversary or its allies are still trying to fathom the situation, devise a policy response and allocate appropriate resources to respond to the aggression. In April-May 2014 in Eastern Ukraine, the Russians used their "unidentified troops" to seize government buildings in Donetsk, Lutansk and Kharkiv; had their separatist allies in Eastern Ukraine declare independence as "People's Republics"; and gathered uniformed troops on the border of Eastern Ukraine in a threat to annex the separatist-controlled territory. This fusion of the instruments of national power allowed the Russians to destabilize Eastern Ukraine and ultimately led to a cease-fire and the retention of territory by Russian separatists backed up by Russian forces. During

this time period, the United States and its allies were not sure (at least publicly) as to the exact nature of conflict in Ukraine. There was widespread suspicion that the Russians were operating in Ukraine but no tangible proof until pictures of suspected Spetnaz soldiers and Russian military equipment were crowd-sourced and identified at multiple locations throughout Eastern Ukraine. Furthermore, the main concern of the US Congress at this point was the massing of Russian troops on the border and not the actions taken by Russians inside the Eastern Ukraine. This is the finest example of Grey-Zone actions moving faster than the bureaucracy can react and difficulty in achieving common understanding of the true nature of the conflict amongst all parties involved.[43]

- **Attack in Five Domains – Land, Sea, Air, Cyber and Information/ Propaganda**. Based on the uniqueness of each situation, aggressors will determine in which domain or domains, they can achieve the greatest leverage in the Grey-Zone. Examples of operations in each of these domains include: Using proxies and criminal networks on land; Using swarms of attack boats or fishermen at sea; Using reconnaissance drones or civilian aircraft in the air; Shutting down electrical grids or conducting denial of service attacks over networks; and finally, using information warfare and propaganda to influence the population. The goal of using all available domains is to fuse multiple tactics and techniques together in a single space and time to strain the opponent's resources and take advantage of where he is weak.[44]

- **Use of Criminal Organizations and Networks**. Aggressors will use criminal networks to create ambiguity, shape public perception and move supplies around the battlefield. Criminal organizations, especially those involved in smuggling and supply of narcotics, have well-connected distribution networks. For a price, Grey-Zone aggressors can use these organizations and networks to supply their proxies, disrupt adversary's operations, disrupt adversary's police forces, and intimidate or coerce target population,[45] e.g., Russia used

criminal networks during its annexation of Crimea and Sergey Valeryevich Aksyonov, the current Prime Minister of Crimea, who is supported by Russian President Vladimir Putin has extensive ties with organized criminal networks.[46]

- **Laws and Cultural Norms as a Weapon System**. In Grey-Zone, aggressors try to use the international law and cultural norms to their advantage. Grey-Zone actors conducting operations with speed and autonomy are able to exploit the bureaucratic processes inherent in these institutions and achieve objectives before these institutions are able to react or decide upon to take appropriate action, e.g., during Russia's actions in Eastern Ukraine, Vladimir Putin openly talked about using Ukrainian citizens to shield Russian troops. Then, they used the unwillingness to fire on unarmed citizens to stage occupations and demonstrations, as well as to seize Ukrainian Army garrisons.[47] Furthermore, once Russian involvement in Ukraine became more overt and Russian actions began to shift to open warfare hybrid tactics, the Russians used legal systems and frameworks such as parliamentary approval of Crimea's annexation to justify their actions.[48]

Conclusion

In the post-Cold War era, the geopolitical conflicts are increasingly being resolved by using non-military means. In fact, the character of warfare has changed with more options for pursuing strategic ends just below the threshold of traditional armed conflict.

Israel-Hezbollah War of 2006 has given rise to the modern concept of 'Hybrid Warfare' but in 2014 Russian actions in Crimea and Eastern Ukraine resulted in the emergence of Grey-Zone. As it is amply evident from its color code, i.e., shade of Grey lies between White and Black; Grey-Zone encompasses the space between peace and war in which aggressors use hybrid tactics to shape the battlefield and achieve strategic objectives short of all-out declared conflict. Some strategic thinkers delineate 'Hybrid Warfare' and 'Grey-Zone' conflicts as two distinct phenomena in international affairs - 'Hybrid Warfare' at tactical level and 'Grey-Zone' conflicts or 'Warfare in Grey-Zone' incorporating

long-term strategic dimensions of the international dispute. They consider 'Hybrid Warfare' as a tactical sub-set of Grey-Zone conflict deployed under certain conditions and varying degrees.[49]

China and Russia know that they cannot compete head-on-head with the United States – economically, militarily and technologically – so they create new battlefields. They engage in Grey-Zone conflict primarily through unconventional techniques with the hope of not only achieving short-term tactical victories against the US and NATO but to challenge the regional and/or global order of alliances and influence international norms of conduct. The United States' electoral system is the heart of the world's most powerful democracy. By selectively amplifying targeted disinformation and misinformation on social media and forging de facto information alliances with certain groups in the United States, Russia arguably won a significant battle without most Americans realizing it ever took place. Thanks to the Russian intervention, Americans are locked in a national argument over the legitimacy of its electoral system.[50] Gerasimov wrote, "The information confrontation opens up wide asymmetric opportunities to reduce the combat potential of the enemy."[51]

Information domain is one of the five domains in which the aggressor can achieve the greatest leverage in the Grey-Zone.

***Brig (Dr.) Rajeev Kumar Bhutani (Retd)** is a Senior Fellow, CENJOWS, New Delhi

References:

1. The Joint Staff, "Joint Publication 1, Doctrine for the Armed Forces of the United States", March 25, 2013., as cited in John Chambers, "Countering Grey-Zone Hybrid Threats", p.8., available at https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Grey-Zone-Hybrid-Threats.pdf
2. Ibid.
3. Gary Anderson, "Counter-Hybrid Warfare: Winning in the Grey Zone", Small Wars Journal, p.1., available at https://smallwarsjournal.com/jrnl/art/counter-hybrid-warfare-winning-grey-zone
4. Misha Ketchell, "Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone?", available at http://theconversion.com/explainer-what-is-hybrid-

warfare-and-what-is-meant-by-the-grey-zone-118841

5. John G.L.J. Jacobs and Martijn W.M. Kitzen, "Hybrid Warfare", 24 April 2019, available at https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0260.xml
6. Frank Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Warfare", Arlington, VA: Potomac Institute for Policy Studies, December 2007, p.14, available at https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
7. Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action", Carnegie Endowment for International Peace, 2019, p.3., available at https://carnegieendowment.org/files/Rumer_PrimakovDoctrine_final1.pdf
8. Nadia Schadlow, "Peace and War: The Space Between", 18 august 2014, War on the Rocks, available at https://warontherocks.com/2014/08/peace-and-war-the-space-between/
9. Frank G. Hoffman, "Hybrid Warfare and Challenges", Joint Force Quarterly / issue 52, 1st quarter 2009, p.35., available at https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf
10. Jonathan Finer, "Israeli Soldiers Find a Tenacious Foe in Hezbollah", *The Washington Post*, 8 August 2006, available at https://www.washingtonpost.com/archive/politics/2006/08/08/israeli-soldiers-find-a-tenacious-foe-in-hezbollah/16ecb81f-c9a7-4500-bad8-dcc24a822174/
11. Andrew Exum, "Hizballah at War: A Military Assessment", Policy Focus #63, Washington, DC: Washington Institute for Near East Policy, December 2006, pp. 8-11., available at https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus63.pdf
12. Matt M. Matthews, "We Were Caught Unprepared: The 2006 Hezbollah- Israeli War", The Long War Series Occasional Paper 26, U.S. Army Combined Arms Center Combat Studies Institute Press Fort Leavenworth, Kansas, pp. 54-55., available at https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf
13. Milton Hoenig, "Hezbollah and the Use of Drones as a Weapon of Terrorism", Federation of American Scientists, 5 June 2014, available at https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism/
14. Frank G. Hoffman, op.cit., p.37.
15. William M. Arkin, "Divining Victory: Airpower in the 2006 Israel – Hezbollah War", Air University Press, Maxwell Air Force Base, Alabama, August 2007, p.29., available at https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0109_ARKIN_DIVINING_VICTORY.pdf
16. Andrew Exum, op.cit., p.5; Matt M. Matthews, op.cit., p.17 (For a complete listing of Hezbollah rocket systems, see Appendix B); William M. Arkin, op.cit., p.31. (20,000 rockets of varying ranges); and Frank G. Hoffman, op.cit., p.37.

17. Charles K. Bartles, "Getting Gerasimov Right", Military Review 96, no.1: 30, January-February 2016, p.30.
18. Mark Galeotti, "*The 'Gerasimov Doctrine' and Russian Non-Linear War"*, available at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/; and Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine", Foreign Policy, 5 March 2018, available at https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/
19. Charles K. Bartles, op.cit., p.34.
20. Miroslaw Banasik, "How to Understand the Hybrid War", Securitologia, No 1 /15, Akademia Obrony Narodowej, Warszawa, p. 28., available at https://www.researchgate.net/publication/285545487_How_to_understand_the_hybrid_war
21. General Valery Gerasimov,"The value of science in foresight: New challenges require rethinking the forms and methods of warfare", Voyenno-Promyshlennyy Kurier online, 26 February 2013, available at http://vpk-news.ru/articles/14632.
22. David Carment and Dani Belo, "War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare", Canadian Global Affairs Institute, October 2018, pp. 6-7., available at https://www.cgai.ca/wars_future_the_risks_and_rewards_of_grey_zone_conflict_and_hybrid_warfare
23. Charles K. Bartles, op.cit., p.34.
24. General Valery Gerasimov, op.cit.
25. Charles K. Bartles, op.cit., pp.34-35.
26. David Carment and Dani Belo, op.cit.,p.7.
27. Ibid., p.7.
28. "Russia May Have Tested Cyber Warfare on Latvia, Western officials say", Reuters, 5 October 2017, available at https://www.reuters.com/article/us-russia-nato/russia-may-have-tested-cyber-warfare-on-latvia-western-officials-say-idUSKBN1CA142
29. David Carment and Dani Belo, op.cit.,pp.7-8.
30. Ibid., p.5.
31. Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, February 1999,available at https://archive.org/stream/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui_djvu.txt
32. "Winograd Committee submits final report", Israel Ministry of Foreign Affairs", 30 January 2008, available at https://mfa.gov.il/mfa/mfa-archive/2008/pages/winograd%20committee%20submits%20final%20report%2030-jan-2008.aspx
33. General Joseph L. Votel et al., "Unconventional Warfare in the Grey Zone", Joint Forces Quarterly 80, 1st Quarter January 2016. P.102., available at https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf
34. "Unified Land Operations", Army Doctrine Publication (ADP) 3-0, Headquarters,

Department of the Army, October 2011, as cited in John Chambers, op.cit., p.10.

35. John Chambers, op.cit., p.13.
36. Ibid., pp. 13-14.
37. Ibid., p. 15.
38. Ibid., pp. 15-16.
39. Ibid., p. 14.
40. Ibid., p. 16.
41. Mari Elisa Dugas, "Between Georgia And Crimea: The Social Dimensions Of War For The Russian Military", April 2016, available at https://repository.wellesley.edu/cgi/viewcontent.cgi?article=1432&context=thesiscollection.
42. Maciej Bartkowski, "Nonviolent Civilian Defense to Counter Russian Hybrid Warfare", The Johns Hopkins University Center for Advanced Governmental Studies, March 2015, p.10., available at https://www.nonviolent-conflict.org/wp-content/uploads/2018/12/GOV1501_WhitePaper_Bartkowski.pdf
43. Andrew Radin, "Hybrid Warfare in the Baltics: Threats and Potential Responses", Rand Corporation 2017, p.7., available at https://www.yumpu.com/en/document/read/57028413/hybrid-warfare-in-the-baltics; Bill Gertz, "Russian Troop Movements Near Eastern Ukraine Trigger Fears of Imminent Invasion", The Washington Free Beacon, 27 March 2014, available at https://freebeacon.com/national-security/russian-troop-movements-near-eastern-ukraine-trigger-fears-of-imminent-invasion/; and John Chambers, op.cit., pp. 17-19.
44. John Chambers, op.cit., pp. 19-20.
45. Ibid., p.20.
46. Simon Shuster, "Putin's Man in Crimea Is Ukraine's Worst Nightmare", Time, 10 March 2014, available at https://time.com/19097/putin-crimea-russia-ukraine-aksyonov/; and https://en.wikipedia.org/wiki/Sergey_Aksyonov
47. Maciej Bartkowski, op.cit., p.9.
48. Nicholas Fedyk, **"**Russian "New Generation" Warfare: Theory, Practice, and Lessons for U.S. Strategists", Small Wars Journal, available at https://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D-warfare-theory-practice-and-lessons-for-us-strategists-0
49. David Carment and Dani Belo, op.cit.,p.2.
50. Molly K. Mckew, "The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare. And it's probably being used on you", available at https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538
51. General Valery Gerasimov, op.cit.

TECHNOLOGY: A SANJEEVANI FOR GREY ZONE WARFARE

Air Mshl PP Khandekar, AVSM (Retd)*

"Above all, always be capable of feeling deeply any injustice committed against anyone, anywhere in the world. This is the most beautiful quality in a revolutionary."

- Che Guevara

When I received a letter about the topic, I realised that technology is all pervasive and has entered everyday life of everyone, almost indistinguishable from the life itself. I also remembered my PG days at NITIE Mumbai in 1987, when I had chosen an elective 'Artificial Intelligence'. Of course, this field was in nascent stage and we had two languages then LISP and Turboprolog. The professor was as novice as we and that made things easier! Technology remains a force multiplier in every sense of the word and I recalled the motto of Military Institute of Technology as "Technology always wins" when I was Commandant and Director; then it was a DRDO Lab. Now it is under HQ IDS and the motto is "Victory through Technology". Well…call it anyway, you may like technology, you may hate technology, but you can not do without technology. A thought that struck my mind was the jargon on Grey or Grey zones of warfare; there also we have difference of opinion on how to spell a simple word! And that brings me to another point. Is this also not grey warfare- USA distorting the British English to reduce the influence and make people adopt and adapt to US way or rather no-British way? Another funny thing about the grey colour is that it can be formed by combining black and white or equal amounts of cyan, magneta and yellow. The yellow-orange-red combo gives "warm" grey while Green-blue-violet combo gives "cool" grey! This colour also represents dullness, loss or depression- not in the warfare however!

Rainbow Colours of Warfare

In today's world success needs to be redefined in politics. Any alternative course of action that can predict substantial gains without reaching the threshold of an armed conflict or a war is welcome. *"Move only if there is a real advantage to be gained*." by Sun Tzu is apt in this grey zone environment. As Carment, Nikolko and Belo suggest, today's geopolitical conflicts reflect a desire by some states to gradually, but fundamentally, revise the regional or global system of alliances and international norms to a degree not even seen during the Cold War. This process of conflict-induced change is known as grey-zone conflict, in which states conduct operations that only occasionally pass the threshold of war. Frank G Hoffman in his book has covered the forms of Statecraft and Influence in the following way:-

Traditional/ Legitimate	**Non-traditional/ Illegitimate**
Security cooperation and foreign military sales	Political subversion by penetration or false-front organizations
Economic sanctions	Economic corruption
Public diplomacy and support for IGO/NGO	Propaganda/psychological operations/ disinformation
Military presence/engagements/ exercises	Cyber intrusions/cyber corruption/ disruption
Foreign internal defence	Sponsored criminal activity
Freedom of navigation exercise (maritime or Aerospace domains)	Electoral interference

He speaks about the continuum in the conflict in the overarching Special Warfare domain, where there are measures short of armed conflict at one end and irregular warfare/ terrorism, hybrid warfare and conventional warfare limited to theatre wide objective at the other end.

'An arrow shot by an archer may or may not kill a single person; but skillful intrigue, devised by a wise man, may kill even those who are in the womb.' 'If the end could be achieved by non-military methods, even by methods of intrigue, duplicity and fraud, I would not advocate

an armed conflict'. 'Any activity which harms the progress of the enemy engaged in similar undertakings is also a progress'.- Chanakya

Grey-zone conflict refers to those post-Cold War conflicts – not always violent – which are prolonged and frequently characterized by an ambiguous point of victory. Grey Zone conflicts are prevalent as ever. It is neither new nor unprecedented nor unbeatable. In our epic Ramayana, the role of Kaikeyee, that of Narad in Mahabharat are just two examples where grey zone warfare existed. The good and the evil fight irrespective of who won had the seeds of grey zones. If one goes into the deep roots of this grey zone, any difference of opinion when stretched to a great extent may get termed as grey zone warfare in simple words. In our families the proverbial relation between mother-in-law and daughter-in-law can be eternal grey zone warfare with the husband perhaps the surviving casualty.

In 2010, China, due to maritime disputes with Japan restricted export of 'rare earth' materials used for computing, sensors, permanent magnets and energy storage. The hacking attack on Sony Pictures Entertainment in 2014 allegedly motivated by North Koreans is testimony to the blurring lines in this grey zone warfare. USSR role in Azerbaijan's crisis in 1946, Indonesia's confrontation with Malaysia over Borneo in 80s suggest practicing grey zone warfare strategies. The Russian Shadow War in the Crimea, the growth of ISIL in the Levant, and the Boko-Harim incursion into West Africa may be becoming the new order of the world. Russia asserting its influence in Ukraine, Georgia, Belarus and Transnistria, China's actions in disputed islands and international waters, the action in Syria where regional players such as Iran, Saudi Arabia, Turkey and Israel with extra-regional powers i.e. USA and Russia competing in grey zone and ISIS use of online videos are all examples of grey zone warfare. Fake news, conspiracy theories, Wikileaks and Julian Assange are all prominent players. It is said that Russia and China follow the philosophy of A2AD- Anti-Access/ Area Denial in the asymmetric environment.

Professor Klaus Schwab, chairman and founder of the World Economic Forum, argues that the collapse of barriers between digital and physical, and between synthetic and organic, constitutes a Fourth Industrial Revolution, promising a level of change comparable to that

brought about by steam power, electricity and computing. The 19th Century Industrial Revolution showed how technological asymmetry can translate into geopolitical inequality – in the words of Hilaire Belloc's poem 'The modern traveller', spoken by a European about Africa: "Whatever happens, we have got the Maxim Gun, and they have not". (The Maxim Gun was the first recoil-operated machine gun). Today, the proverbial Maxim gun is the technological asymmetry, proliferation of groups with advanced capabilities and acute sense of injustice to individual or a group of people that are well equipped to wage a grey zone warfare. Sanjeevani is the magical herb-technology in today's world garnished with cyber, that will give the wherewithal and new life to the non-state as well as state actors to influence the politics at all levels. It will also act as a shot in the arm for the now extinct risings against the State and those in deep slumber or the sleeping cells. A report by McAfee and think tank CSIS pegs the figure to US $ 400 billion as the cost of the cyber crimes all over the world. It amounts to combined defence budget of European Union or Asia region.

Today's geopolitical conflicts are marked by collaborative efforts by groups re-orienting themselves against a common enemy and set up new rules of the game in the area of dominance and influence. To take three of the most potent weapons – information, credit and capital – these used to be monopolised by the same powers that possessed superior firepower and moral authority, namely the US and its allies. That is no longer the case. The weapons, the power and the narratives are more disparately distributed. Frank Hoffman coined the term Hybrid warfare in the context of Hezbollah fight against Israelis in 2006. Hybrid warfare can be a tactical subset of grey-zone conflict deployed under certain conditions and in varying degrees. Hybrid warfare mostly operates in tactical level while grey-zone conflicts employ and deploy all available instruments of power transcending international borders in creation of a dispute and sustaining it. A formal definition of grey zone tactics is offered by Hoffman as, "Those covert or illegal activities of non-traditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage." As Dr Geraint Hughes puts it, a stable and

predictable military balance can be suddenly overthrown by innovative doctrines or cunning strategies in this milieu due to technological asymmetry. Major differences in the two approaches are given below:-

Characteristic	Grey-Zone Conflict	Hybrid Warfare
Level	Tactical, operational, strategic	Tactical and operational
Use of conventional military operations	Used alongside non-conventional operations.	Used alongside non-conventional operations. Usually the dominant element.
Use of non-conventional military operations	May be used stand alone or alongside conventional operations.	Used alongside conventional operations as auxiliary tactics.
Protracted engagement	One of the dominant characteristics.	May be protracted or short.
Global and/or regional revisionist ambitions	One of the dominant characteristics.	Out of scope as the concept pertains to operational and tactical levels.
Symmetry between opponents	Used under both symmetric and asymmetric conditions.	Largely used under asymmetric conditions.

China is using its capital and extending its credit on a scale previously unimaginable, and the strategy is paying dividends. Russia has become the most subversive player in cyber space, while China is helping itself to Western IP. It is no surprise that in this new ranking competition is tough and unsettling for those who used to dominate, and it feels sufficiently hostile to be a war.

Though grey zone conflicts are complex in their character, reach and effect, militarily speaking, there are some basic steps that could be defined to fight this warfare. Literature on Special Operational Forces of USA suggests that the Tactics and Operational Art to apply to Grey Zone Conflicts Are:

- Doing with less; extremely limited resources
- “Boots on the Ground” restrictions
- Department of Defence NOT in the lead
- Whole of Government nested Military Indirect/ Surgical Strike approach
- The ability to advise and assist indigenous proxies/ forces
- Regional expertise and language capability
- Extreme or “in extremis” negotiations
- Extended periods of time in the Grey Zone
- Intelligence based operations for precision Targeting/ Force Protection
- Accepting there will be no defined military victory

I am sure, the mandarins at HQ IDS and the service headquarters with the Intelligence agencies are working on the doctrine, philosophy and execution in this new era of invisible enemy, within and without.

Technologies

“Studying technology without consideration of how it might be employed in the future divorces means from ends and risks putting the proverbial cart before horse.”

Human nature essentially has not changed and history has shown that any technology developed with moral façade has been used to develop some sort of weapon and new technologies are no exception. New technologies are overcoming the adverse atmospheric, land, sea and air/ space conditions to be applied in the four dimensions including time. The ubiquity of innovators especially in the democracies gives more chances of technologies going in the hands of few algorithmically driven social media groups or a group of individuals in them crossing national barriers transcending and permeating in all layers of societies to promote radical views and wage an asymmetric warfare with tangible gains and conduct influence operations. The larger question will be out of the State and the private players, who considers himself a master of technologies or a slave of technologies.

The new arms race is all pervasive with 70 nations and more launching satellites and nano satellites in space, the fight of dominance in the information domain and developing new networks for command and control. The field of Artificial Intelligence has opened new vistas in deep sea as well and information technologies. Augmented humans/ leaders, robot-human teams, remote killing machines, Lethal Autonomous Weapons and Systems (LAWS), are just a tip of the iceberg on the reality that one watched in movies a few years ago. On the other hand, though the concept of fission bomb was understood in physics, to bring it to reality needed a lot of money, infrastructure, skill sets and long gestation period. Thus even today this technology has remained with a few nation states and has not seen proliferation in the hands of private players wanting to fight an asymmetric warfare. Uber`s recruitment of a team of robotics researchers from Carnegie Mellon University in 2015 is an example, which decimated the research effort they had had been working on for the United States department of Defence. Disruptive technologies may offset this barrier for non-state actors to dominate.

"Increased use of automation also has the potential to increase the pace of warfare. An accelerated tempo of operations (for both machines and people) and the OODA loop may lead to combat that is more chaotic but not necessarily more easily controlled."

As envisioned in a recent future-casting workshop, warfare will continue to be transformed by advances in information technologies. In fact, information itself will become the decisive domain of warfare. Four developments will significantly change the nature of the battle. They are Proliferation of intelligent systems, Augmented humans. the decisive battle for the information domain and the introduction of new, networked approaches to command and control. Each of these new capabilities possesses the same critical vulnerability - attacks on the information, communications and computers that will enable human-robot teams to make sense of the battlefield and act decisively. Hence, the largely unseen battle for information, communications and computer security will determine the extent to which adversaries will be able to function and succeed on the battlefield of 2050.

It is possible to carry out innovations in genetic engineering in a basement. As Patra and Andrew explain, the repercussions of using

a viral vector to carry a new functional gene is still unknown and could have negative impacts on the human body. Some processes involve the use of antibiotic-resistant genes, which can ultimately be lethal. The Chinese have produced a dog which, through genetic modification, has twice the muscle mass of a normal dog. Another key biotechnology trend tied to human machine teaming is work with BCI that enhances wireless data transfer between humans and machines and ultimately among humans. This technology, although not currently deployed, could ultimately link capabilities and other technologies via thought. BCI could enable new approaches to performance assessment, as well as performance enhancement and training. Although research in this field is in early stages (in the lab), efforts continue toward enabling more-efficient prosthetics, wireless system control, wireless transfer of data between human brains, performance enhancements, and performance assessment. Other such fields are synthetic biology, big data and machine learning in virtual world. It is therefore difficult to fathom how these technologies intersect and how and what the effect will be. Killer robots, Laser weapons, advances in Genetic innovations, Behavioural science, chat-boats, are some of the pointers of technologies making their way in every field. Genetics innovator Balaji Srinivasan has envisioned “Silicon Valley`s ultimate exit” from the USA. Paypal co-founder Peter Thiel has floated the idea of establishing a sea colony to literally offshore himself from government regulation. Elon Musk has talked about colonising Mars. There is serious interest in businesses formulating their own foreign policy. Technology will make this possible.

Bitcon or block chain innovation has opened the doors of authentication, anonymous transfer of funds reliably and in a secured way. Quantum computing technologies will allow hackers to intrude highly secured networks. Bitcon having military applications makes it double use technology. Chinese aggression defines the “ambiguity — about the ultimate objectives, the participants, whether international treaties and norms have been violated, and the role that military forces should play in response.” The uncertain nature of grey zone warfare is what makes blockchain so appealing as a tool. Adversarial governments and extremist groups can utilize it – with little fear of being caught “red-handed” – to further their interests at the expense of other countries unwilling or unable to stop it. Due to lack of clarity of law enforcement

agencies this technology will allow less prepared nations to be worried about the wide gap with better prepared nations and non-state actors. This in turn will generate more inequality cascading it into grey warfare intensifying.

Michael O'Hanlon, a Technology forecaster in his book on Forecasting changes in Military Technology 2020-2040 has studied 29 technologies that interact to bring changes in 38 systems and associated infrastructure and facilities. There are seven systems under Sensors, eight under Computers and Communications, twelve under Projectiles, Propulsion and Platforms and 11 under Other Weapons and Key Technologies. They are as follows:-

Technologies	Levels of Changes		
	Moderate	High	Revolutionary
Sensors			
Chemical sensors		X	
Biological sensors		X	
Optical, infrared, and UV sensors	X		
Radar and radio sensors	X		
Sound, sonar, and motion sensors	X		
Magnetic detection	X		
Particle beams (as sensors)	X		
Computers and communications			
Computer hardware			X
Computer software			X
Offensive cyber operations			X
System of systems/Internet of things			X
Radio communications	X		
Laser communications		X	

Artificial intelligence/Big data			X
Quantum computing		X	
Projectiles, propulsion, and platforms			
Robotics and autonomous systems			X
Missiles	X		
Explosives		X	
Fuels	X		
Jet engines	X		
Internal-combustion engines	X		
Battery-powered engines		X	
Rockets		X	
Ships	X		
Armor		X	
Stealth		X	
Satellites		X	
Other weapons and key technologies			
Radio-frequency weapons	X		
Nonlethal weapons		X	
Biological weapons		X	
Chemical weapons		X	
Other weapons of mass destruction	X		
Particle beams (as weapons)	X		
Electric guns, rail guns			X
Lasers			X
Nanomaterials			X
3D printing/Additive manufacturing			X
Human enhancement devices and substances			X

The terms moderate, high and revolutionary are subjective and somewhat imprecise. In general terms, technologies showing moderate advances might improve their performance by a few percent or at most a couple of tens of percent—in terms of speed, range, lethality, or other defining characteristics—between 2020 and 2040. Those experiencing high advances will be able to accomplish tasks on the battlefield far better than before—perhaps by 50 to 100 percent, to the extent improved performance can be so quantified. Finally, technology areas in which revolutionary advances occur will be able to accomplish important battlefield tasks that they cannot now even attempt. The above assessment gives some idea of applications in these 29 technologies interlaced intricately as the innovators galore. He expects revolutionary changes to take place in six technologies as can be seen from above, mainly in cyber domain. There is enough evidence to suggest that unless there is a breakthrough in technology following pearl curve or S curve, his assessment by and large is correct.

Conclusion

"…it ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new.

— Niccolò Machiavelli

Sanjeevani is that magical herb to cure neuro problems and lengthening the life line. Laxman was injured and Hanuman got Sanjeevani. Today Sanjeevani i.e. advances in technologies with special reference to ICT and AI domains yet to be explored in entirety, are seemingly available to private sector more than the state organisations, especially in the democracies due to resources and intelligentia distribution. There are many Laxmans arising everyday from the hurt caused by actions of many, due to the sense of injustice and wherewithal available to address the same. Ram are the state actors who may/ may not get support from such Laxmans, though there will be other set of Laxmans furthering the progress of the society by positive means, as for every technological problem, there is a solution. There are enough Ravans to create ripples/

turbulence/ unrest in the minds of the peoples. Only time will tell who gets genuine Sanjeevani and how it is put to use.

"War is a force that gives us meaning."

- Chris Hedges

***Air Mshl PP Khandekar, AVSM (Retd)** is former Air Officer in-charge Maintenance, Air Headquarters, New Delhi.

References

1. Javier Jordan. It is not a new Cold War: they are grey zone conflicts.
2. David Carment and Dani Belo. War's Future: The risks and rewards of Grey Zone conflicts and Hybrid Warfares.
3. John Raine. War or Peace? Understanding the Grey Zone.
4. Dave Betz. Grey zone conflicts may be the new normal, but will have the same marginal success.
5. Michael E.O'Hanlon. Forecasting changes in military technologies.
6. Alexander Knott, David S. Alberts, Cliff Wang. War of 2050: A battle of Information, Communication and Computer Security.
7. Anja Kaspersen, Espen Barth Elde, Philip Shelter- Jones. Article based on World Economic Forum project on relationship between fourth industrial revolution and international security.
8. Blog comments by Bill M, Dr Gerant Hughes et al.
9. John D. Winkler, Timothy Marter, Marek N Pazard, Raphel S Cohen, Meagen L Smith. RAND corporation project on Reflections on the Future Warfare and Implications for Personnel Policies of the US Department of Defence.
10. Frank G Hoffman. Examining complex forms of Conflict: Grey Zone and Hybrid Warfare.

PSYCHOLOGICAL WARFARE: A CORNERSTONE OF GREY ZONE WARFARE

Lt Gen PJS Pannu, PVSM, AVSM, VSM (Retd)*

A Single assassin can achieve, with weapons, fire or poison, more than a fully mobilized army.

-Kautilya

General

The world watched the killing of Iran's General Qassem Soleimani in Baghdad by the US drone attack on Friday, 03 January 2020. While American spokesperson initially denied the American involvement, Trump justified it as elimination of Number 'One terrorist', saying that he had sanctioned the attack to "stop the War". In response, the US bases in Iraq were hit with rockets and missiles the following days, with Iran announcing that the country would take 'blood for blood' revenge at a time and place of Iran's choosing.

The elimination of Osama Bin Laden, Bagdadi, Saddam Hussain, Gadaffi whether heads of sovereign states or heads of declared terrorist outfits are only few to name in the endless list of acts of war, but certainly lie outside the understanding of regular warfare. In such kind of warfare, the means do not have to justify the ends or ends do not justify the means. The 'might' is of the 'impact' on population and the terror it creates. Place and time of killing, methodology of killing and the justification of it have no conventions. Similarly, acts such as 9/11, 26/11, attacks on Indian parliament or drone attacks on the oil targets in Saudi Arabia are all acts of War but are outliers in the definition of conventional warfare.

Definition

'Grey Zone Warfare' is a form of irregular warfare persecuted by either irregular forces or by regular troops in the garb of irregular groups or in

collaboration with irregular armed groups to achieve strategic / national objective by forcing their will on another nation. In such situations, the victim or the responder takes long to comprehend the complexities. This environment creates uncertainty and fear among the target nation who cannot hit back or counter attack due to ambiguity in the existence of the persecutor. Since the nations/organizations in these operations do not use full military might or overt conventional Military, these situations have been traditionally termed as a situation of 'No War No Peace', 'Operations Other than War' or 'Less Than War Scenarios'

In the 'grey Zone' one major consideration is deniability – 'it never happened' or we 'did not do it' or make tall claims for creating a psychological impact. This kind of warfare is an outcome of many conditions - When the nations are uneasy with one another and diplomatic solutions been exhausted, the conventional forces cannot be used either due to devastation and economic losses or because of deterrence of WMD (Weapons of Mass) Destruction. In other words when the nation states want to use coercive or 'gun-boat' diplomacy without direct use of Military, and resort to using asymmetric means of war which appears formless, can be defined as Grey Zone Warfare.

One of the prime understanding of Grey Zone is that neither the attacker nor the victim is clearly definable. Governments of the country shall not know whether the trigger was external or internal and which agency should respond and in which way? The trigger of the attack or a problem are camouflaged through diffusion so that no one agency and no one solution can be identified as a fix. Use of targets would be in multiples and would mostly lie in the overlap of responsibilities. Complexity and chaos are the recipe of Grey Zone.

'Grey Zone' in the Indian Context

In India this situation is generally described as 'half front' in the contextual understanding of Warfare. The expression of 'half' needs elaboration as this does not have a benchmark or a relative understanding of 'full'. India being a peace-loving nation, practices Non-Alignment or strategic autonomy, has invested in peace (Shanti), a concept given by the father of Nation, Mahatma Gandhi. India has traditionally seen Warfare more in the shades of 'Black' or 'White' rather than 'Grey'. India has fought

four Major Wars, over disputed land borders, maintains large standing conventional force and Special Forces. The country has faced constant Insurgency and Proxy War situations ever since its independence. India has been fighting Insurgency and Proxy war by employing conventional forces. Kargil conflict was a border war where Indian regular forces fought with the Pak units fighting concealed under the garb of irregulars. Our regular units have also experience in Sri Lanka and Punjab where serious lessons were drawn. Our Army personnel have contributed very effectively in Special Groups and National Security Guards (NSG) in handling Hijack situations and preventing attacks on civilian population. The Police ably trained by the Army has been fighting Left Wing Extremism (LWE). By any measure, Special Forces and regular infantry units have not been fighting in the grey Zone but have been drawn into conditions similar to it. 'Half' front is seen from a perspective that the forces will have to continue to fight Proxy War and Insurgency at the same or more intense levels even during the hot war and protect own Lines of Communication.

What would Grey Zone mean in the Indian context? Firstly, Indian troops have been actively engaged on the Line of Control to prevent infiltration by Pak terrorists. In combination with active LC, our troops have engaged in Counter Terrorist Operations in the hinterland. Both type of operations are on own territory. The terrorists' training Camps, leadership, recruitment etc. are all based on foreign soil and people of Pakistan and Pakistani Army support them materially, morally and direct operations. Till the time our response to Proxy War is about operating on Indian soil, we are not fighting a grey Zone battle but merely protecting own territory, life and property. This is a reactive process. However, there has been a paradigm shift in the Indian doctrine when India began hitting across the borders. The surgical strikes by the Special Forces and the airstrikes by the IAF are application of regular combat power in an undeclared war. However, use of media and Information/disinformation campaign in support of such operations takes us into the fringes of grey Zone. In the Indian context the narrative is certainly undergoing a change. With the increasing use of technology, cyber, space, Special forces in the changing nature of Warfare gives a clear pointer that Indian Forces have to prepare, train and operate in the Grey Zone. There has to be a mandate shift which is seen on the anvil with the raising of the AFSOD.

Certain characteristics and ingredients that effect the changing nature of warfare to the Grey Zone is discussed in the succeeding paras.

Human Mind

The action of Operators, groups or force that operate in the Grey Zone is heavily dictated by the influences of a human mind. There is a huge variation in means and methodology every time a group conducts an operation. This form of warfare is devoid of templates or SOPs. Operations are likely to be highly innovative, ingenious and unpredictable. The tempo of operations too is flexible. There can be long periods of lull when the groups can go into hibernation, and then make sudden change in threshold levels of violence ranging from phycological to non-Kinetic to highly volatile levels. The Grey Zone warfare is as complex as the human mind.

The Grey Zone Wars are heavily depended on psychological Operations. The narratives are orchestrated and changed with rapidity to create chaos. The combination of violence and disinformation are part of the same battle rhythm. The human mind is a prime target in addition to life and property. The success is not measured by gains or losses of real estate, but dislocation of people's minds and force migrations. The targets are not always military, but certain military targets are hit to discredit the Military power. Some soft military targets include families of military personnel, logistical installations, lines of communication etc. Taking hostages or assassination of Military and political leadership is usual.

The Indian Forces have to operate in a large canvas and multiple fronts. Two major adversaries in the West and North have little in common in their character but their collusively makes 'half front dynamics' unique. The Forces have to operate in all forms and circumstances. Our forces have suffered more casualties in undeclared wars than in declared wars. Every event, place and time of operational engagement is different from the past. The Non-Kinetic and Non-Contact element is likely to increase as part of warfare. The cyber-attacks on critical infrastructure, popular sites and social media attacks would lie in the grey zone where the responsibility of various agencies overlap. In India many agencies and ministries deal with security, cyber issues, and critical infrastructure

security. Military would not know how to deal with it due to mandate overlaps and fault lines, however would get drawn into responding to these issues.

Nations at Peace are at War

The global world order is constantly shifting. This is an outcome of constant struggle and quest of Nations to grow their economies, trade, business, industry, technology and military power. There is a constant competition to outdo the other. Even though world idolizes peace and overtly works towards it in a seemingly collaborated way, there are always undercurrents generated by this competition. Countries have their own interests that come first and need to be protected. The trade competitions, barriers, sanctions and coercive diplomacy etc. bring about a friction that manifests in many overt or covert actions that a nation may indulge. Suspicion necessitates gathering, protecting and manipulating information, undercover intelligence and espionage. Conspiracy becomes a necessary, yet unstated part of practicing diplomacy. While Nations appear to be at Peace are constantly at War. In a way there is always a part of 'Grey Zone' (not War Yet) that remains at the foundation of overtly peaceful coexistence of nations.

Pakistan has been at War with India since its inception; however, India has never declared/ been at war with Pakistan but drawn into it. All Wars were initiated by Pakistan with a belief that India shall neither retaliate or capture Pakistan territory. Possession of Nuclear Weapons, has emboldened Pakistan to fight Proxy War including grab actions. She has practiced a strategy of bleeding India. Pakistan goes to any extent of using diplomacy, collusive arrangements, information campaign, propaganda, active use of terrorists, triggering civil unrest and any form of direct and indirect action to 'bleed India'. Pakistan Military runs the deep state which has kept itself at war with India in perpetuity, while keeping the regular Military out of the conventional war zone.

Deterrence is the Key to Shift

The trend world over is moving away from use of conventional forces. The 'force on force' engagements are things of the past. Any future warfare would have 'asymmetry' built into a War Winning Strategy. Initially, large

conventional force disparities could be offset by building WMD capability, to ensure disproportional superior conventional forces of one country do not run over the inferior force of another. Pakistan and North Korea have been able to achieve such a strategy of deterrence effectively. It is known that WMD are not meant for war fighting. However, 'nuclear blackmail' and 'sabre rattling' as demonstrated by these nations have proven credible. Infact, the chances of success of grey zone operations enhance when backed by WMD.

While Pakistan and China both maintain conventional forces and possess WMD. Pakistan Army keeps the LC active through exchange of fire as a diversionary tactics in support of terrorists to infiltrate, as also to internationalize borders as disputed. On the other hand, China keeps pushing PLA patrols across the LAC, jostling with Indian troops to keep their territorial claims alive. Pakistan is already operating in the Grey Zone and maintains and operates a large number of irregular and terrorists' forces. China has not used the grey Zone along the LAC as their relations with Tibet are not conducive and is conscious that playing Grey Zone with India would seriously upset their plans of assimilating Tibet in the long run.

Violence is Endless/Unrestricted, Intermittently Uneventful

The Grey Zone has no identifiable beginning and no visible end, it has enough evidence of its presence, yet no one event is so prominent that would define it in a particular manner. Such type of warfare may have differing intensities but not one form. This form of warfare may tire out a nation but not the players who persecute operations. The response to Grey Zone would remain in the Grey Zone and its discourse can materially change with the change of leadership or ideology.

The last major battle was fought with Pakistan in 1971 and later in 1999 a limited border war was fought at Kargil. Similarly, the last conflict with China was in 1962. However, a deep look into events would suggest that we have been fighting an endless war, yet major events can be counted on few figures. The Force levels of Armed Forces have doubled since last major wars. Forces like Rashtriya Rifles have added a major force muscle. Similarly, the sharp increase in Border Guarding Forces, CAPFs, Para Military Forces, etc. has taken place in the last

two decades. In spite of phenomenal increase in Force levels, the overall threat to the nation has not subsided. The internal and external challenges have been on the rise. Each Leader/VVIP finds an increasing need for security cover, including some of our missions abroad. There is a certain indicator, that our country has been and is being increasingly drawn into the Grey Zone.

Technology Makes Existing Concepts Redundant

Since technology is increasingly aiding or replacing human effort, so is it doing to a combatant at an exponential rate. The current Industrial revolution 4.0 has brought about Accelerated Transformation in Military Affairs. The future Warfare would be digital and Non- Contact. The priority of targets would shift from destroying forces to disablement and dislocation of forces. It is easier to bring down a critical Infrastructure of a nation through a Cyber Attack. The forms and tools employed for Surveillance and Targeting would enable a force of private warriors to have access to information, monitoring, analysis, detection and destruction which would be outsourced to a machine. The state sponsored groups and the Special Forces are increasingly using dual strike capabilities using combination of technology and human effort for Recce and Direct-Action. Use of Mini and Micro UAVs controlled by satellite makes third dimensional special operations very effective.

A study on ‘use of technology by Non-state Actors’ at the Directorate of Defense University IDS had brought out a number of lessons. In more than many ways it was established that the irregular groups are much quicker in raising and utilizing funds, more flexible and adaptable to technology and generally ahead in learning and operating curve. Procurement of hardware through dark web and organizing funds is convenient without leaving a trace. Innovative use of crypto currency, dark web and social media with nimble footedness makes them very potent in conducting Grey Zone Operations. These are being innovatively used by ‘Pakistan deep State’ in fighting proxy war.

Challenging World Order – Unease at all Levels

The friction is more visible in the top competing countries of the world. Generally, the P5 are seen as an exclusive club, not fighting direct wars,

however they are participating in the battles against each other at a third place. Case in point is Syria, Yemen, Iraq, Afghanistan etc. where operations are conducted under the garb of fighting GWOT or against regimes which support differing ideologies. Similar competition and contests manifest in the less powerful blocks with in grey zones coming up all over the world in varied forms.

Even though India and Pakistan cannot not be equated, unfortunately for India, they get clubbed together in the international fora due to a slugfest of blame game. India must continue to punch according to its weight and get its rightful place on a higher table. India has practiced strategic autonomy but many times, had to take an ambiguous position. India has been asked to participate in the GWOT in places like Afghanistan and Iraq or Pick sides on issues between two nations etc. This has been a challenge as we could not be perceived to be taking sides due to our interests and not seen to be fighting in the Islamic zone of conflict. India wants to take a 'Black or White' approach. As a result, our understanding and investment in the areas of Grey Zone is absent or at best negligible.

Battles of the Future – Will we need Armies

The changing forms and norms in warfare makes one think, as to what would be the role of future Armies? or would we need Military for conventional roles at all? Would it not be sufficient to just guard borders aided with smart fences and AI applications? The Border Guarding Forces braced with technology would ensure sanctity of frontiers. Certainly, nations having no assets of deterrence would need conventional capabilities. The conventional military attacks would be checkmated by the WMD for those who have them. If that be the case, who would respond to terrorist threats or Grey Zone attacks?

Indian Army has been reorganized into Integrated Battle Groups (IBGs) for fighting in the Nuclear overhang. This would make it possible for large force levels to be applied at multiple points making broad but shallow territorial gains where retaliation with WMD would not be justified. Pakistan on the other hand has pre-empted any type of aggression by declaring the policy on use of tactical nuclear weapons by lowering the threshold of tolerance. Would this mean that India's strategy of response

to Pakistan's Proxy War by a shallow capture of territory has already been checkmated? This draws us into finding answers to Proxy War responses in the Grey Zone. One of the outcomes of Grey Zone is that it throws war fighting concepts and doctrines into the cycles of irrelevance.

Flexibility is the Order - Monolithic Structures are a thing of the Past

It is a popular belief that if an organization has to survive it must be based on solid structures believed to be sustainable. The SOPs, templates, rules, regulations, and structures are antithesis for units that operate in the Grey Zone War. While the Governments of the day ensure that such organizations do not become ghosts that come back haunting and turn a liability to the authority of the nation, yet there are compulsions that would necessitate building certain units without which the Nation may even face a larger or even an existential threat.

Pakistan has heavily invested into the Jehadi Forces. These forces are very nimble and flexible. Every Major War fought by Pakistan, whether in India or Afghanistan has been either supported or wholly fought by the irregular forces. Pakistan has made sense of the chaos, with the backing of the WMD and has preferred to operate below the conventional Military level. In spite of them openly supporting and running terrorist operations, nations like US were compelled to make them allies in the GWOT. Even China, being mindful of threat from Muslim fundamentalists and their emerging threat has supported Pakistan militarily. US has lately branded Pakistan as an unreliable partner, but has not withdrawn their support. Pakistan continues to use these forces in traditional areas.

Role of State

It is a myth that most of the groups that operate in the Grey Zone are Non -State actors. These groups, more often than not, operate as part of the 'deep state'. Deep State can be defined differently in different countries. The Special Forces or a nominated covert group of the nation, may be given a mandate. Many countries hire Private Military Companies/ mercenaries for such high-Risk Missions. Those troops may operate along with conventional Forces and at that time need not be run by the 'deep state', however,these troops with Special mandate would have

least signature but deep roots. Many international bodies with light foot print are known to be collaborating in such operations for supporting common interests.

The nations who have been collaborating on the GWOT, have signed formal arrangements of intelligence sharing and cooperate. These arrangements are also made when regular troops of countries cooperate in collusive manner such as ISF in Afghanistan and similar arrangements are made between forces to fight ISIS. However, of necessity, troops or groups operating in the Grey Zone land up being fiercely independent and may land up in a situation of fighting directly against the Government backed adversary groups. There has been a swell in the employment of Private Military companies which have come up in a big way.

Role of Special Forces

Every country has a component of Special Forces as part of Military or Para Military Force. Even though they are formed units and equipped to a military specification, the organizations hugely differ from country to country. The flexibility and adaptability are the edifice of SF organizations. Such forces are very easily prone to be interfaced with the other forms of warring organizations, whether regular or irregular. The members of Special Forces are most adaptable and you cannot set too many templates for them to operate. Similarly, the equipment profile, training, and organization would be flexible for being suitable for application for multi domain, multi terrain and Hybrid situations. Even though no organization is 'Fail Safe' yet it must have high degree of assurance of success in an ambiguous environment and promise of sustainability.

The Indian Armed Forces have been maintaining traditional Special Forces with their respective services. Army has SF battalions, Navy has Prahar units and IAF Garud units. Each one has a tailor-made role to operate with respective services domain in support of conventional operations. In some measure these units can operate bi-service or Tri-service depending on the operational necessity. With the raising of the Armed Forces Special Operations Divisions (AFSOD) which is a tri-service formation, it is better equipped, organized and tasked for operations that shall fall beyond the charter of the traditional

SF units of the three services. The mandate given to them shall dictate their employment suitability in the Grey Zone.

Conclusion

The Special Forces of the Armed Forces or forces under mandated agency has to be ready to respond to any eventuality that is complex, sudden, and highly violent. Such groups need to be trained, equipped, organized and mandated to carry out operation in ambiguous environment. The 'tooth for tooth' and 'eye for eye' reaction must be sharp, immediate and punitive, both declared and undeclared wars. This can only happen if the concept of Grey Zone is understood and practiced. During Hot War situation the SF should be prepared to operate behind enemy lines and achieve interoperability with groups or other units operating in the Grey Zone.

***Lt Gen PJS Pannu, PVSM, AVSM, VSM (Retd)** is a former DCIDS (DOT), HQ IDS, New Delhi

INFLUENCING ELECTIONS: GREY ZONE WARFARE

Maj Gen Umong Sethi, AVSM, VSM (Retd)*

For democracies, elections are a fundamental constitutional instrument that enables an orderly and peaceful transition of governing polity. They also decide the next main decision maker and composition of coalitions or alliances, if any. The new regime might bring about shifts in a country's domestic and foreign policies and re-chart its international behaviour. Even in case of authoritarian regimes, world has seen many rulers loose power as a consequence of a fair election. Flowing from that, new dispensation that followed can bring about fundamental changes to the existing governance system and the manner in which the country interacts with rest of the world. This immense power of elections to shape future course of events in a country, its neighbourhood and world at large incentivises big foreign powers to try and influence outcomes in favour of a party or an individual.[1]

According to Wikipedia, foreign electoral interventions are both covert and or overt attempts by big powers to influence elections in another country. There are many ways that nations have accomplished regime change abroad and electoral intervention is only one of those means.[2] Theoretical and empirical research on the effect of foreign electoral interventions was not extensive until 2011. Since then, a number of very insightful studies have been conducted.[3.] Intervening in elections of other countries is not a recent phenomenon. Research shows that between 1946 and 2000, United States of America and USSR/Russia intervened 117 times to influence outcomes of elections of other countries. That in effect constituted interventions in in about one of every nine competitive national-level elections during the period. Of the 117 interventions, United States share is 81 followed by Russia (including the former Soviet Union) at 36.[4] Their methods ranged from providing funding for their preferred side's campaign to public threats to

cut off foreign aid in the event of victory by the disfavoured side. Majority of those interventions (68%) were through covert, rather than overt actions. A 2019 study by Lührmann et al. at the Varieties of Democracy Institute in Sweden summarized reports from each country to say that during 2018, most intense interventions, by means of false information on key political issues, were by China in Taiwan and by Russia in Latvia. The next highest levels were in Bahrain, Qatar and Hungary. Lowest level interventions were in Trinidad and Tobago, Switzerland and Uruguay.[5] [6] [7]

Studies on foreign intervention in elections have theorized two types on interventions. First, 'partisan intervention', where the foreign power takes a stance on its support for one side. The second is 'process intervention', where the foreign power seeks to support the rules of democratic contest irrespective of who wins. These interventions can be specified as globally or self-motivated depending upon the intended outcomes in terms of promoting interests, betterment or well-being. The agents of interventions are likely to be nation states, international organizations, non-governmental organizations and individuals.[8]

Dov H. Leven in an elaborate study, 'Effects of Great Power Electoral Interventions on Election Results' argues that, overall, 'partisan electoral interventions' seem to substantively benefit the aided candidate or party. He goes on to infer that for a great power to intervene in an election in another country, there are two conditions that must be met. These are, compelling 'motive' to do so and an 'opportunity' to intervene. Motivation stems from the big power perceiving its interests being endangered by a certain candidate or party to the extent that it makes conventional responses of incentives and disincentives to resolve disagreements appear potentially ineffective or too costly. As far as opportunity is concerned, a significant domestic actor must consent to willingly cooperative with proposed electoral intervention by the great power. Without the domestic actor's cooperation in providing information and local knowledge about the electorate's preferences and the best ways to intervene in its favour, the great power will usually see its chances of succeeding as too low to justify an electoral intervention. In the absence of either one of these conditions, the great power is unlikely to intervene in the elections in most cases. Another conclusion of the study suggests that while its accepted that interventions do swing

elections, an intervention is not likely to take place if the potential client is likely lose the election despite the intervention.[9] There seems to be a consensus among scholars that for the foreseeable future, partisan electoral interventions will continue to be an option and effective way for great powers to determine the leadership of other states.

In recent years, technology has quite radically impacted all aspects of human lives. Tools are available to gauge human behaviour and predict choices they are likely to make. Learning from marketing companies that target customers by analysing roughly 300 data points to know exactly who their customers are and what are their established behaviour patterns to impact buying choices, election managers now use the same techniques to profile their voters and effect their voting preferences. Reliance is placed on 'Big Data' analytics, Artificial Intelligence (AI), Machine Learning (ML), intelligent algorithms and autonomous bots to engage with voters far more effectively than hither to fore by creating voter psychographic and behavioural profiles. Cambridge Analytica, the organization that allegedly secured victories for both Donald Trump and the Brexit Leave campaign, had created 220 million personality profiles for adults in the United States alone, using up to 5,000 data points.[10] Focused advertising campaigns based on profiling are targeted to specific voter or groups to influence voting choices. The impact of such an endeavour resulted in influencing voter turnout on the day of UK's general elections in 2017.[11] US midterm elections in 2018 saw the advent of 'Deepfakes'. Deepfakes are audio or video messages generated by AI which shows someone saying or doing something that they did not say or do. To counter Deepfakes and fake news, bots are employed to detect the misinformation being spread. The same can then be red flagged to minimise influence.

Brookings in a report entitled, 'Malevolent soft power, AI and the threat to democracy' as a part of series "A Blueprint for the Future of AI," analysed new challenges introduced by artificial intelligence and other emerging technologies. Its findings state, 'while the internet can still mobilize large numbers of people to political action, it can also spew false information about candidates, suppress the vote, and affect the voter rolls and the election machinery of the state. By 2016, social media had become a weapon against democracy as opposed to a tool for democracy.'[12]

Brookings study mentions, “fact of Russian interference in the 2016 election is now well known in the United States. What is less well known is that the Russians have been at this in other countries; from elections in the Ukraine, to the Brexit vote in Great Britain, to Scotland, Austria, Belarus, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Moldova, Montenegro, Netherlands, Norway and Spain.”[13] It goes on to suggest that the purpose of Russian interference was deeper than attempting to move the election in a particular direction preferable to Russia. It was to destroy faith in democracy by making citizens doubt the electoral system. The report alleges that the Russians stole the ‘Clinton campaign’s’ internal modelling to target voters and used it to suppress the vote amongst African-Americans and to alienate Bernie Sanders’ voters from Hillary Clinton. They allegedly used “Blacktivist” and the “Woke Blacks” accounts and masqueraded as ‘African-American’ and ‘Muslim activists’ to urge minority voters to abstain from voting in the 2016 election or to vote for a third-party candidate.

An article in ‘The Atlantic’ lists ways to interfere in American elections without violating the existing law. Some of the findings suggest measures to include, exploitation of already deployed state-run news organizations. In that, engagement of state-supported news organizations like RT, Sputnik. China Daily, and Al Jazeera and the like to infuse political agenda into run-of-the-mill journalism. The international news agencies can advocate openly or clandestinely in favour of and against candidates or parties. Second, to run political advertisements online. Most democracies do not have regulations to control foreign financing for online campaigns and advertisements and this can be exploited. Governments and non-state actors can use fake news, disinformation campaigns, and networks of bogus accounts on the social network to distort domestic or foreign political sentiment to achieve a strategic and or geopolitical outcome. AI & ML tools along with social media and political espionage can be used as possible instruments to further the misinformation pursuits. Third, funnel money through a non-profit organisation. These groups have stated objective of ‘social welfare’ but, could be used for political purposes to influence election outcomes. Quoting example of Pope Francis, the spiritual leader of roughly 75 million Catholics in the United States, pronouncing during the 2016 presidential campaign that building the kind of border wall that

Trump had championed was "not Christian" amounted to a foreigner breaking with diplomatic protocol and exerting influence on election in the most basic way. That was another way of swaying electoral outcomes.[14] These methods with a few modifications can be applied against any other democracy to influence elections there.

Dov H. Leven's study "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results" mentions that in 1977 Indian parliamentary elections, the Soviet Union intervened in favour of Mrs Indira Gandhi and the Congress party. The intervention was covert was not able to prevent, or even soften the crushing blow it suffered from the Janata party. The Soviet intervention is estimated to have assisted the Congress party in only around eleven seats or so. The assessed impact on vote swing was approximately two percent. This number was too small to have any serious effect on the election results given that the Congress party lost more than 150 seats in this election and the Janata party won 295 seats and an absolute majority in the 542-seat Lok Sabha.[15] The episode highlights that even when number of seats targeted are small its unlikely that desired outcome can be achieved especially when it's a wave in favour of the opponent. Another aspect that stands out is the incorrect assessment made by the Soviets to intervene in a case where the intended beneficiary had little chance of success and in any case the intervention was of a very limited scale to make an impact. If the intervention came to the notice of the next government and what impact it had on the relations if any, needs further examination to establish effect of failed intervention on international relations.

As per reports, India has about 250 million active Facebook and 400 million WhatsApp users. Add to that, India has over 800 million mobile phone users had the benefit of cheapest mobile internet services in the world till recently. Facebook's WhatsApp has been extensively used in all recent domestic elections. While many messages were ordinary campaign missives, some were intended to inflame sectarian tensions and others were downright false with no way to trace where they originated. The role WhatsApp played in influencing voters has received far less attention globally than that of its sister services Facebook and Instagram. Both Facebook and Instagram had come under intense

scrutiny in recent months for how Russian agents used them to manipulate American voters in the 2016 presidential election. WhatsApp has largely escaped that notice because it is used more heavily outside the United States, with people in countries like India, Brazil and Indonesia sending a total of 60 billion messages a day.[16] Technogically Indian voters are well connected and fairly active on social media. It is easy to profile and target them to affect their electoral choices. This holds outwardly true when examined in light of digital campaigns by various political parties during state and national elections.

Srikanth Kondapalli, Professor of Chinese Studies at the Jawaharlal Nehru University, is of the view that with increase in trade and investments by China, a causal link among business influence, political parties and electoral funding is slowly emerging. According to him 'China factor' is becoming increasingly explicit in the Indian context. Ever increasing millions of netizens in India use extensively Huawei, ZTE, Xiaomi, Vivo, Oppo and products of other mobile phone companies. Many of these have operating systems based in China and that could provide some leverage for China in years ahead. Android apps designed and produced by Chinese companies are extensively used countrywide. Hikvision, a Chinese company has bagged orders from various government agencies in India, including Airport Authority of India, Central Coalfields and forces employed in counter insurgency operations for providing electronic surveillance equipment like CCTV cameras and access control gadgets. No conclusive study is available to confirm if it creates some vulnerability that can be exploited during elections.

It is well known that nations influence the perceptions via social media in targeted countries through data harvesting and by other means. China has enough footprint in India to embark on similar missions as in few other countries. Kondapalli makes a telling point that after the 2017 decision of the 19th Communist Party Congress in Beijing to occupy the "centre stage" in global and regional orders and to export the "China model" to other countries, Beijing is likely to pursue aggressively selling its story in other countries. This involves not only soft power but also monitoring and influencing the cyber-domains in other countries.[17] There is thus a need to study this aspect of foreign influence in greater detail

to arrive at safeguards and pre-emptive measures to guard sanctity of electoral processes.

Democracies must take measures to protect themselves against foreign powers attempts to influence outcomes of elections. To that end a few suggestions are offered. First, re-visit regulations to regulate social media. Its easier said than done as it invokes serious and often partisan debate questioning freedom of press, expression and the like. However, post Facebook public hearings both in US and in Europe, there is fair degree acceptance of at least social media platforms sharing information about persons or groups spreading malicious propaganda. Though, this will require great deal of consensus building and is difficult but, efforts need to be made to make progress in this regard. Second, is to strengthen institutions. Institutions like the Election Commission need to be strengthened by giving them access to various tools and means including trained skinware to detect, isolate and take action against any malicious attempts to intervene in or influence electoral outcomes. Legal issues in this regard will also have to be looked into and addressed. Any organisation is as good as the people who man it and to that end people with impeccable integrity and character should be appointed to such high offices. Political parties are an important stakeholder in the system. Unambiguous protocols must be laid out and any violation of collusion with any foreign agency of organisation will invite immediate sanction. As has been mentioned above, a foreign power is unlikely to attempt influencing elections without collusion of a group contesting elections. Third, the intelligence community must use its human intelligence and new technological tools to focus on the IT sector to keep track of and prevent serious interference in the democratic processes. Lastly, creatively designed voter education programs to help them recognize the differences between fact and rumour, news and advertising, news and opinion and bias and fairness must be planned and executed. Advocacy should be strengthened by bringing to light fake news stories. A discerning citizenry is the best assurance against foreign interventions.

***Maj Gen Umong Sethi, AVSM, VSM (Retd)** is a well known, Delhi based Defence Analyst and Author

References:

1 When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results Dov H. Levin International Studies Quarterly, Volume 60, Issue 2, June 2016, Pages 189–202, https://doi.org/10.1093/isq/sqv016 Published: 13 Feb 2016 https://academic.oup.com/isq/article/60/2/189/1750842 accessed on January 21, 2020 at 11.10 AM

2 https://en.wikipedia.org/wiki/Foreign_electoral_intervention accessed on January 21, 2020 at 11.00 AM

3 https://en.wikipedia.org/wiki/Foreign_electoral_intervention accessed on January 21, 2020.

4 Levin, Dov H. (June 2016). "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results". International Studies Quarterly. 60 (2): 189–202. doi:10.1093/isq/sqv016. For example, the U.S. and the USSR/Russia have intervened in one of every nine competitive national level executive elections between 1946 and 2000. https://academic.oup.com/isq/article/60/2/189/1750842 Retrieved on January 21.

5 Democracy Facing Global Challenges, V-DEM ANNUAL DEMOCRACY REPORT 2019, p.36 (PDF) (Report) 14 May 2019 accessed on January 24, 2020.

6 Su, Alice (16 December 2019). "Can fact-checkers save Taiwan from a flood of Chinese fake news?". Los Angeles Times. Retrieved January 24, 2020 at 10.17 AM.

7 Kuo, Lily, and Lillian Yang (30 December 2019). "Taiwan's citizens battle pro-China fake news campaigns as election nears". The Guardian. ISSN 0261-3077. Retrieved January 24, 2020 at 10.18 AM.

8 Wikipedia Foreign Electoral Intervention https://en.wikipedia.org/wiki/Foreign_electoral_intervention accessed on January 21, 2020.

9 When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results Dov H. Levin https://academic.oup.com/isq/article/60/2/189/1750842 accessed on January 24, 2020 at 10.42 AM.

10 Jacob Bergdahl, 'How AI Can Make You The President', for politicians aiming for a higher seat of power, there is an immense power in understanding artificial intelligence-technologies—no matter the ethics, Jun 4, 2019 https://towardsdatascience.com/how-ai-can-make-you-the-president-4756f6b1c0c0 accessed on January 18, 2020.

11 Manu Siddharth Jha, How AI and Machine Learning Can Win Elections Dec 17, 2019 https://www.mygreatlearning.com/blog/how-ai-and-machine-learning-can-win-elections/ retrieved on January 19, 2020.

12 Elaine Kamarck, BROOKINGS, 'Malevolent soft power, AI, and the threat to democracy' Thursday, November 29, 2018 https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy/

13 Ibid. Quoting 'Way, Lucan Ahmad and Casey, Adam. (2018, January 8). Russia has been meddling in foreign elections for decades. Has it made a difference? The Washington Post. Retrieved from https://www.washingtonpost.com; Casey, Adam; Way, Lucan Ahmad. (2017). Codebook - Russian Electoral Interventions - 1991-2017. Retrieved from https://doi.org/10.5683/SP/BYRQQS

14 Uri Friedman, 5 Ways to Interfere in American Elections—Without Breaking the Law. To influence U.S. politics, foreign governments don't have to hack one party and collude with the other. July 24, 2017 https://www.theatlantic.com/international/archive/2017/07/legal-ways-interfere-election/534057/ accessed on January 24, 2020.

15 Levin, Dov H. (June 2016). "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results." Pp200. https://academic.oup.com/isq/article/60/2/189/1750842 Retrieved on January 21.

16 Vindu Goel, 'In India, Facebook's WhatsApp Plays Central Role in Elections' https://www.nytimes.com/2018/05/14/technology/whatsapp-india-elections.html May 14, 2018 retrieved on January 20, 2020.

17 Srikanth Kondapalli, China's influence on the elections in India China's economic clout is transforming - slowly but surely - into political leverage https://progressivepost.eu/debates/next-global/chinas-influence-on-the-elections-in-india retrieved on January 20, 2020.

CYBER AND ELECTROMAGNETIC ACTIVITIES (CEMA) IN THE GREY ZONE

Brig (Dr) Navjot Singh Bedi*

Preamble

The Grey Zone is a metaphorical state of being between war and peace; the conflict marks an extension of hybrid warfare into the space between war and peace. It employs both conventional and unconventional methods to achieve political goals, as well as ambiguity to cloud the judgement of adversaries. Here 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. The 'zone' essentially represents an operating environment in which aggressors use ambiguity and leverage non-attribution to achieve strategic objectives while limiting counteractions by other nation states.[1] The attributes of ambiguity anonymity and lack of attribution are ideal for the Cyber & EM Activities (CEMA) to take place in the Grey Zone. Grey zone activity is most effective when malign activity is executed within legal boundaries so as not to set off any alarms or cross traditional warning trigger points.[2]

Background

The relentless pursuit of new military technologies by States continues to yield expanding lists of technology-related issues for lawyers to consider in applying the law of armed conflict in complex battlespaces on land, on sea, in air, in space, and in cyberspace. Foremost among these issues is the challenge presented by the principle of proportionality, requiring military forces to refrain from causing excessive damage to civilians and civilian objects when attacking military objectives.[3]

In the late 90's the world has seen a convergence in telecom and Information Technology (IT), with telecom products being developed on computer platforms and multiple applications converging into a single device. The boundary lines between telecom and IT started

blurring and the term Information Communication Technology (ICT) gained currency. With the advent of smartphones and tablets, mobile technology has integrated a number of these technologies with the abilityto transmitwirelessly. In fact the term Infotainment (Information with Entertainment) is slowly gaining acceptance and smart phones with wider screens are in vouge.

In mobile phones, there are no distinct data and voice channels. The introduction of voice over IP (VoIP) protocol though allows voice to be carried over the data networks, yet has a major drawbacks as this form of communication is susceptible to both EW and standard network attacks. Thus now in mobile phones, it is feasible that data-based attacks can impact the voice channels. Mobile phones, especially those with high processing power often double up as a mini computers and have replaced laptops. Mobile phone is a wireless device and is the preferred internet gateway. That's why most of the exploits planned by hackers are targeted towards a mobile phone platform instead of a computer. Therefore logically it is thus therefore susceptible to exploitation of the Electro Magnetic (EM) spectrum.

This article explores the possibilities of conducting Cyber & EM Activities (CEMA) in the Grey Zone, with specific reference to military ICT networks.

General

When the first host-to-host message was sent across the ARPANET in October 1969, few could have fully anticipated the degree to which the internet, and now the internet of things, would explode across the globe and revolutionize nearly every facet of public and private life. Nor could anyone have predicted the degree to which it would establish an entirely new realm—cyberspace—through which States could engage in traditional, and not-so-traditional, statecraft and conflict.

States have fully embraced cyber operations as a means to pursue their national interests and gain low-cost asymmetric advantages over their adversaries. Cyberspace has become a new instrument of statecraft and presents novel and challenging questions about the applicability of existing legal orders.[4] Adversaries are leveraging and exploiting

the numerous technical, policy, and legal ambiguities surrounding cyberspace operations to conduct a range of intrusive and increasing aggressive activities. While some of these cyber operations have been conducted as part of ongoing armed conflicts, the vast majority have taken place in the so-called grey zone—the far more uncertain space between war and peace.

ICT by it's inherent attributes, is able to integrate operations more effectively, provide decision support and thus an overwhelming degree of simultaneity can be achieved. If optimally utilized, ICT can fundamentally change the both the manner of conduct and the outcome of military operations. New and emerging Cyberspace and EM Spectrum (EMS) threats first made their presence felt in the wars in Iraq and Afghanistan. Insurgents actively used the internet both for communication and for propaganda. At the same time, they skilfully used weapons enabled by the EM Spectrum, especially radio controlled Improvised Explosive Devices (IEDs) or RCIEDs. All over the world cyber warfare is now being acknowledged as the 5th dimension of warfare (after Land, Air, Sea and Space). Due to the overlapping realms of Cyber and EM Activities (CEMA), especially in the Grey Zone, the effect of CEMA needs to be analysed, with specific reference to military ICT networks, as the same has the potential to tilt the balance of power.

With the connectivity becoming increasingly wireless, the network technology is moving towards IP for all services. As per the TCP/IP Model on which the whole data communication process relies, the IP Layer ie layer 3 and the layers above were the standard cyber warfare gateway. However now, with the proliferation of wireless technology, the means to access & infect a computer network are now also available at physical layer in the form of Radio Frequency (RF) linkages. Hence simple RF level brute force jamming can be optimally exploited. With the advent of 5G and Internet of Things (IoT), the situation is getting more complicated. Technologies like mobile phone, satellites, wireless backhaul radios, software defined radio (SDR) etc are vulnerable to cyber attacks through wireless channels.

Convergence Between Communication and IT

With the advent of technology, multiple applications have converged into singular devices, and the boundary lines between communications

and IT have started blurring. This convergence has also given rise to the commonly used term ICT. Modern day smartphones are capable of providing voice, data, video services, besides providing functions like calculator, camera, radio, news, entertainment, scanner, web browser, navigational aid, internet hot spot and so on. Mobile phone is however a wireless device and is the gateway to the internet. It is therefore susceptible to exploitation of the EMS, to carry out traditional EW functions, or to carry out cyber warfare.

Most of the telecom equipment, be it a router, a switch, or an IP radio is mostly being provided as a software service over a computing platform. Even telecom hardware based systems like telephone exchanges and satellite etc are being managed through computer systems. The Combat Net Radio (CNR) is also now migrating to Software Defined radio (SDR), which provides an opportunity to carry out cyber warfare through exploitation of RF spectrum. Satellite phones, surveillance devices, cellular phones, and trunked radio systems are also being used by the modern soldier in battle field. All these use a wireless access point and are thus vulnerable to cyber warfare through exploitation of EMS. This changed battle field ICT environment gives both sides enough opportunity to exploit EMS for conduct of operations. With the imminent advent of Internet of Things (IoT), the situation is likely to aggravate further because if IoT is to succeed, it has be wireless. This is likely to expand the scope and reach of cyber warfare and that of our vulnerability to the same, as it's effects are not likely to be limited to the classical battlefield but are likely to permeate into the living rooms of common citizens. Boundaries are being blurred and cyber warfare which was historically associated at strategic level (in state level conflicts) is now available at tactical and operational levels also. Correspondingly, traditionally civil services like banking, transportation, communications, power supply etc being target by CEMA, the common citizens sitting in the hinterland , will also be drawn into the conflict and will be connected to the outcome of the actions at the battlefield level.

EW, Cyber & CEMA in Recent Grey Zone Conflicts

Grey Zone Activities. Such activities include disinformation campaigns, political or economic coercion, cyber operations, activity in space, and proxy support and provocation by state-controlled forces.[5] As real-world

examples, the report specifically cited China's island-building activities in the South China Sea, Russian campaigns to influence elections, North Korean cyberattacks on businesses such as Sony, and Iranian support of militant groups that provoke enemy forces while Tehran maintains plausible deniability. These tactics include everything from propaganda and disinformation to election interference and the incitement of violence.[6]Hybrid adversaries exploit this stabilizing function of the law in order to gain a military advantage over their opponents. They do so by failing to meet the relevant normative expectations, by using a range of means, including noncompliance with the applicable rules, by instrumentalizing legal thresholds.[7]

EW in Grey Zone Conflicts. Though it might not have been used in a synergized manner yet both Cyber and EM activities have independently had a major role to play in some of the major conflicts of the last three decades. This concept of conflict is best illustrated by Russia's actions in Eastern Ukraine in 2014. Grey Zone doctrine leverages ambiguity to create an environment in which adversaries are unable to make strategic decisions in a timely and confident manner. The importance of EW in the conduct of a modern air war was amply demonstrated in the Gulf War as the advanced Iraqi Integrated Air Defence System completely collapsed within a few hours, never to recover to even a semblance of functionality. [8]

Application of Cyber Ops in Recent Grey Zone Areas

In 2007 Russia launched another Grey Zone operation that navigated the fine line between war and peace. The denial of service attack that crippled Estonia in April of that year was the result of tensions between the two countries boiling over. For many people 2007 was when cyberwar went from the theoretical to the actual, when the government of Estonia found itself under a furious digital bombardment that knocked banks and government services offline. Russia did not employ an armed response, which would inevitably invoke Article 5 of the North Atlantic Treaty. Instead, a new kind of deniable operation was used, which lent itself to the grey zone: a cyber operation. Moreover, the DDoS attacks on Estonia did not create physical damage and, while a significant event, were not considered to have risen to the level of actual cyberwarfare.

However, the Idaho National Laboratory proved, via the Aurora Generator Test, that a digital attack could be used to destroy physical objects -- in this case a generator. The Stuxnet malware in 2010, which proved that malware could impact the physical world. Since then there has been a steady stream of stories: in 2013 the NSA of USA said it had stopped a plot by an unnamed nation to attack the BIOS chip in PCs, rendering them unusable. In 2014 there was the attack on Sony Pictures Entertainment, blamed by many on North Korea, which showed that it was not just government systems and data that could be targeted by state-backed hackers. In Dec 2015, hackers managed to disrupt the power supply in parts of Ukraine, by using a well-known Trojan called Black Energy. In March 2016 seven Iranian hackers were accused of trying to shut down a New York dam in a federal grand jury indictment.

Nations are rapidly building cyber defence and offence capabilities and NATO in 2014 took the important step of confirming that a cyber attack on one of its members would be enough to allow them to invoke Article 5, the collective defence mechanism at the heart of the alliance. In 2016 it then defined cyberspace as an “operational domain” -- an area in which conflict can occur: the internet had officially become a battlefield. Cyber warfare is going to be a significant component of every present and future conflict. Future wars will also be fought by hackers using computer code to attack an enemy’s infrastructure, as well as troops using conventional weapons like guns and missiles. But unlike standard military attacks, a cyberattack can be launched instantaneously from any distance, with little obvious evidence in the build-up, and it is often extremely hard to trace such an attack back to its originators. Modern economies, underpinned by computer networks that run everything from sanitation to food distribution and communications, are particularly vulnerable to such attacks, especially as these systems are, in the main, rarely designed to be secure against hackers.

Thus digital attacks against vital infrastructure-like banking systems or power grids - give attackers a way of bypassing a country’s traditional defences. A digital attack which turned off the power, or water, or stopped banks from functioning could be just as disastrous for a sophisticated economy, as a missile strike. The worst case cyberattack scenario could involve outright destructive attacks, focused on some aspects of critical infrastructure coupled with data manipulation on a

massive scale. For eg shutting down the power supply or scrambling bank records could easily do major damage to any economy. And some experts warn it's a case of when, not if.

Application of CEMA in Recent Grey Zone. Though in 2007, cyberwar had actually became a reality when the banks and government services of Estonia were knocked offline, yet it was on 06 Sep 2007, with the launch of Operation Orchard, that CEMA was employed. It which was probably the first time a converged EW and Cyber effort had taken place in modern warfare. Operation Orchard comprised of an Israeli airstrike on a suspected nuclear reactor in the DeirezZor region of Syria, which occurred just after midnight. The attack pioneered the use of the Israel's cyber & EW capabilities, as Israel Air Force systems took over Syria's air defense systems, feeding them a false sky-picture for the entire period of time that the Israeli fighter jets needed to cross Syria, bomb their target and return.[9,10]. Possibly Digital Radio Frequency Memory [11] (DRFM) technology was used to feed misleading information to the Syrian air defence radar system. [12] Similarly, the Russia-Ukraine conflict in 2014 adequately demonstrated the converged operations effect of Information Warfare (IW) tools.

Commonalities Between EW And Cyber Warfare

Operational Function. In both EW and Cyber Warfare, an endeavor is made to listen to enemy EM transmissions to determine his capability and Electronic Order of Battle. Both are primarily tools for gathering intelligence, though the means may differ. Both the domains of activities interfere with enemy's operational capability ie Electronic Attack in case of EW and Computer Network Attack in case of Cyber Ops.[13] Both EW and Cyber Warfare aim to protect friendly capability from enemy's interference; whether be it in the form of Electronic Protection or Computer Network Defence. Another important function of both these domains of warfare is Deception ie to cause enemy systems/ people to take wrong decisions. Thus we see commonality in the Operational Function of both these activities. This is besides the fact that the set of people who plan and execute EW and cyber operations are primarily ICT engineers, with domain knowledge of ICT; in absence of this base knowledge of ICT, conduct of operations in these domains is not possible. Thus we see that there are considerable similarities in these two domains of warfare.

Technology. As regards technology, both EW and cyberspace operations are complementary and multiply the effect of the other. In addition both use wireless communication platforms , networking, digital platforms integrated with computers. EM spectrum is used as a medium to exchange information between computers and this brings in the possibility of intrusion into a computer through EM spectrum. EW weapon systems are now being developed on computer platforms and are no longer discrete electronic based systems. Few examples of these latest genre of EW systems are SDR, and DF systems. Traditionally EW targeted enemy communication systems- through EMS and the Cyber Warfare used to target enemy computer networks. Due to CEMA, the dividing lines between these two are blurring and more often than not their roles overlap.

CEMA Initiatives By The Major World Powers

Chinese PLA. The Chinese IW strategy called "Integrated Network Electronic Warfare" (INEW) consolidates the offensive mission for both CNA and EW. This was earlier under the under 4th Department (Electronic Countermeasures- ECM) of PLA General Staff Department (GSD) but has now been shifted to Strategic Support Force (SSF), that centralizes most PLA space, cyber, electronic, and psychological warfare capabilities. The SSF combines assorted space, cyber, electronic, and psychological warfare capabilities from across the PLA services and its former General Departments. INEW outlines the integrated use of EW, CNO, and limited kinetic strikes against key command and control, communication and computers nodes to disrupt the enemy's battlefield network information systems. [14] The PLA sees cyber warfare as a first-strike option to preclude the requirement of conventional military operations, and not as a force multiplier to conventional operations. [15]

Russian Defence Forces. The Russian offensive into Ukraine in 2014, was an effective integration of Cyber, EW and intelligence with kinetic measures to actually create the desired effect . Russians basically shut down all the military systems, and the Ukrainian soldiers used their cell-phones, and they got located and destroyed. This Russian-style integration of cyber/ EW, drones, and high explosive is a case study in CEMA and could possibly be the way future wars would be fought. As per a statement of Russia's Defence Minister Mr Sergei Shoigu in

the parliament in 2016, Russia plans to form a new branch of its armed forces to focus on information warfare.[16]

Australia Defence Forces (ADF). In Australia, the Cyber and EW Division (CEWD) undertakes "research and development focused on identifying, analysing and countering threats to Australia's defence and national security through electronic means". It integrates science and technological capability across Cyber, EW, SIGINT, and communications to cover continuum of the cyberspace and EM environment. The division applies its capability to support situational awareness of the Cyber and EM environment through reliable and resilient cyber and EW systems including trustworthy ICT, survivable communications networks and systems integration.[17]As per the Strategic Plan 2016-2021 published by CEWD: [18] "wireless network characterisation and vulnerability research" has been listed as a priority area of investment under the Cyber Sensing and Shaping chapter.

US Defence Forces. The US Army and Navy have recognized the need for Cyberspace-EMS alignment and have organizationally aligned their services' cyberspace and EMS operations. The US Army has published the "Army Cyber-EM Contest Capabilities Based Assessment",[19] and the Navy has published the "U.S. Navy Information Dominance Roadmap 2013-2028".[20] Both these publications highlight convergence of cyberspace and EMS capabilities in the future. US Army has disbanded its EW division, and incorporated the same into a newly established Cyber Command at the Pentagon. [21] Under the Integrated Cyber and Electronic Warfare program (ICE), the U.S. Army's Communications-Electronics Research, Development and Engineering Center (CERDEC) is working to identify ways to combine EW capabilities with cyber warfare tactics and enable rapid deployment of new and improved capabilities.[22] US Army Field Manual, FM 3-12 titled "Cyberspace and EW Operations".[23] emphasizes the need to carry out integrated CEMA operations in all phases of war. The US Navy has a concept of EM Manoeuvre Warfare, which also aims to integrate cyber, jamming, spoofing, and careful manipulation of electronic signals to blind and baffle enemies. The US AF has however not aligned its efforts in cyberspace operations with its EW[24] and EMS operations missions in a way that effectively and holistically leverages the EM spectrum and cyberspace to their greatest potential.

Israel Defence Force. Israel are the world leaders in this domain, especially the EW. In Jun 2015 Israel announced that it will raise a unified cyber command, but later, in May 2017 it shelved the plans[25]. The IDF (Israel Defence Force) Strategy-2015 document [26] mentions electronic warfare in the passing and includes the need for developing cyber warfare capabilities [27].

Indian Defence Forces. The "Joint Doctrine For Electronic Warfare: 2010" published by HQ IDS, Ministry of Defence (MoD) is an important document which lays down the doctrinal concepts in Information Warfare (IW)/ EW domains. It is recognized that overwhelming advances in improved communication, information, surveillance, reconnaissance capabilities and net-worked command & control elements, must be gainfully exploited to fight ahigh-tech warfare. However no serious convergence between EMS and the cyber warfare has actually taken place.

Options Available. CEMA synergizes diverse capabilities across various domains of war fighting. It has the potential to optimally utilize complementary effects of various domains of war fighting through cyberspace and the EMS. If the Armed Forces are to have a modicum of success, it will be imperative to dominate cyberspace and the EM Spectrum will become more complex and critical to mission success. Proliferation of 5G and IoT is likely to throw up multifarious challenges in managing the already congested frequency spectrum. Thus in order to obtaining and maintaining freedom of action in cyberspace and the EM Spectrum, while denying the same to enemies and adversaries, it will be necessary to incorporate CEMA not only in all ops of conventional warfighting and throughout all phases of an operation. This will be even more relevant during the Grey Zone due to the inherent features of lack of attribution, deniability and ability to transcend geographical boundaries.

Exploiting CEMA in the Grey Zone

Electro Magnetic Pulse (EMP). EMP first came into prominence as one of the fall outs of a nuclear explosion and it was this phenomenon which triggered the need to establish a type of communication which could continue to work in the aftermath of a nuclear explosion. Consequently the Advanced Research Projects Agency Network

(ARPANET) was developed, which an early packet-switching network and the first network to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet. EMP is also sometimes called a transient EM disturbance, is a short burst of EM energy. EMP interference is generally disruptive or damaging to electronic equipment, and at higher energy levels a powerful EMP event can damage even physical objects such as buildings and vehicles. It is actually the first classical example of CEMA, because on account of a short burst of EM energy, communication systems & computers are rendered non effective by burning the electronics inside. Weapons have been developed to deliver the damaging effects of high-energy EMP. Tactical EMP weapons would affect a small area and could be used to create a devastating effect on the enemy, neutralizing the power grid, communication systems, traffic light systems etc and create chaos.

TEMPEST. Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions or TEMPEST is a U.S. National Security Agency specification and a NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. It is a project of the NSA of USA [28] was conceived to address the issues of data leakage through unintended EM radiations and the protection against it. It is one of the first areas in which work had commenced on exploitation of CEMA. Unintended EM radiations from digital devices, such as those from the computer/TV screen, data cables, electric cables, keystrokes, etc can be monitored and the content can be reconstructed [29]. TEMPEST monitoring equipment includes various kinds of sensitive receivers, which can monitor a wide range of frequencies, and a combination of hardware and software that is capable of processing the received signals into the original data, typically works across few 100 meters of distance between the target machine and the receiver.

Mobility & Wireless Connectivity. In addition to EMP and TEMPEST, the exploitation of CEMA in the Grey Zone, especially for cyber warfare can be facilitated primarily in a fluid battle field environment requiring extensive mobility as this mobility in turn demands wireless connectivity. The same is equally applicable in civil or in military networks/ applications/devices and this will be even more relevant during the Grey

Zone as the conventional military safeguards and defenses are down in a peacetime environment and lot of opportunities present themselves for exploitation of EM Spectrum for cyber warfare. This can be undertaken in the following ways:-

(a) Conventional hacking of WiFi networks

(b) Aim to capture raw RF signal and analyse it offline to extract information

(c) By infiltrating a computer network and injecting it with malware to c arry out cyber attack.

(d) To re-feed a doctored RF signal back into the system for deception etc.

(e) Man-In-The-Middle (MITM) Attack

(f) Post injection with a malware, to force the system to transmit data to external devices using covert channels.

Hacking WiFi Networks. This is possibly the most commonly used activity that can be conducted during the Grey Zone and involves getting access to data through the traditional wireless connections like the WiMAX, wireless IP radios, Wi-Fi, Bluetooth, air interface of the cellular connection (cell phone to the tower), etc. This is another reason why it's a good idea to avoid using free unsecured public WiFi networks or for that matter even unsecured public charging points for mobile phones/ laptops.

Malware Injection using Drones. Using Drones, malware can also be injected over the wireless channel. It is more easily done in the open channels and is a slight challenge if the wireless channel is encrypted. This can pose to be a serious challenge due to the easy availability and low cost of drones. The rapid advancement in the miniaturization of drones and their enhanced suite of applications for civil commercial use has added a new dimension to this threat, which makes it an ideal vector for exploitation during the Grey Zone using CEMA. Another dimension is that Drones can also be controlled remotely so whoever controls CEMA can control the drones. However counter measures against such technologies are already in place.

Digital Radio Frequency Memory (DRFM). It is an electronic method for digitally capturing and retransmitting RF signal. DRFMs are typically used in radar jamming, although applications in cellular communications are also becoming common, which makes it an ideal candidate for exploitation during the Grey Zone using CEMA. A DRFM system is designed to digitize an incoming RF input signal at a frequency and bandwidth necessary to adequately represent the signal, then reconstruct that RF signal when required. As a digital "duplicate" of the received signal, it is coherent with the source of the received signal, and there is no signal degradation; thus a significant obstacle for radar sensors. With radars being used in not only the aviation industry but also in railways and in maritime shipping, the payoffs on employing CEMA for DRFM related activities are humongous and can cause untold misery and chaos in the intended target nation.

Man-in-the-Middle (MITM) Attack. A DRFM system can also be used to conduct a so-called man-in-the-middle attack (MITM) against a targeted RF receiver. This attack vector has immense potential especially in the banking and financial sector, and the normally secured channel of communication used for authentication can be easily compromised and funds can be siphoned off in a matter of seconds from an unsuspecting adversary. The military applications of this are only limited by imagination. In an MITM attack, an attacker has the ability to alter traffic in a communications channel by injecting themselves into the communications channel between the transmitter and intended receiver. Since the bits can be manipulated, the target receiver can be fooled either through preamble/ synchronisation bit manipulation (that will cause loss of synchronisation) or by manipulating the traffic bits (which will cause receiver to get a garbled/doctored message) [30].The US Army and Navy are already using DRFM systems (from M/s Mercury Systems, USA) to bolster their intelligent jamming and deception capabilities [31,32].

Capture EM Signatures. DRFM-based systems can also be used to capture the EM signatures of enemy aircraft, ships and other units; these EM signatures can provide intelligence about the capabilities of enemy aircrafts, ships and types of electronic systems in operation. This is an ideal activity that can continue during the Grey Zone and the data base built up can be optimally utilized during times of hostilities. The

technology is catching fast and the global market valued at USD 614 Million in 2016, is projected to reach USD 1,222 Million by 2022 [33].

Penetration of Air Gapped Networks. Few important organisations the Indian Army, store and process classified sensitive information within their computer networks which are 'air-gapped' to prevent a breach, so that there is no physical/ electronic connection between secure PC and one connected to the internet. A cyber researcher, at the Ben Gurion University in Israel, Mr Mordechai Guri, has however devised ways to exfiltrate computer data to another nearby device using various methods. However, the assumption that Mr Guri makes is that the computer is already infected with the customised malware, through a USB drive etc. Various methods to exfiltrate computer data to another nearby are:-

(a) Via the noise its internal fan generates,

(b) By changing air temperatures in patterns that the receiving computer can detect with thermal sensors,

(c) By blinking out a stream of information from a computer hard drive LED to the camera on a quadcopter drone hovering outside a nearby window [34].

Disrupt CNR / Citizen Band Radio/ GPS Reading. During the Grey Zone period, CEMA can be effectively employed to enter an SDR network of the adversary, using spoofed IP, and meddle with control signals to disrupt the CNR of Armed Forces (being used for Exercises/ Training/ Practice Camps), or disrupt the Citizen Band radio being used by the police and other agencies or to even send misleading messages to enemy soldiers or display false GPS reading. The last one ie false GPS reading has the potential to cause major chaos because these days nearly everyone travels using some form of GPS aided navigation assistant (for eg Google Maps).

Conclusion

Development of technology has enabled exploitation of CEMA, especially in the Grey Zone as it can provide disproportionate gains associated with overt military aggression, without crossing the threshold of open

warfare with a powerful adversary. CEMA provides an ideal operating environment in which ambiguity and non-attribution can be leveraged to achieve strategic objectives while limiting counteractions by other nation states .The fact that military networks in the tactical battle field are primarily wireless, makes the employment of CEMA even easier and feasible. With the impending advent of 5G and IoT, an even larger target space is provided for CEMA. 5G and IoT will also proliferate in military networks in times to come, thus enhancing the scope of employability of CEMA.

In an era where all wireless protocols are well defined and the information is available in public domain, CEMA finds great applicability as it is simpler to design hacks for them. Hacking encrypted channels pose a tougher challenge but solutions are there for such networks. US Army uses a spy drone Wireless Aerial Surveillance Platform, or WASP. It measures over sixfeet in length and wingspan has been modified to make it more useful for hacking by equipping it with the tools to crack Wi-Fi network passwords. WASP can also act as a GSM network antenna enabling it to eavesdrop on calls/text messages made over that network by any phone deciding to connect through it [35].

Due to advancement in technology, current commercial off-the-shelf (COTS) DRFM systems are capable of receiving analog signals, converting them to a digital signal, processing and manipulating the digitized signal at the bit level, and converting the modified signal back to an analog signal for transmission in less than 39 nanoseconds [36]. The threat of CEMA is real and will be a game changer if optimally employed in the Grey Zone. Cyber operations are an unconventional tactic that has been and will continue to be used in grey zone approaches by adversaries and CEMA further compounds the challenge. It is equally important to understand that we are equally vulnerable to CEMA and need to protect the EM Spectrum and Cyber space through intelligent use of technology and innovative thinking.

***Brig (Dr) Navjot Singh Bedi** is a BGS(TT), HQ ARTRAC, Shimla

References

1. MirosławBanasik, http://journal.dresmara.ro/issues/volume7_issue1/04_banasik.pdf.
2. Warning for the Grey Zone by Lindsey Sheppard and Matthew Conklin; Mark Voyger, “Russian Lawfare – Russia’s Weaponisation of International and Domestic Law: Implications for the Region and Policy Recommendations,” Journal on Baltic Security 4, no. 2 (2018), https://content.sciendo.com/abstract/journals/jobs/ahead-of-print/article-10.2478-jobs-2018-0011.xml.
3. https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-9 ; The Principle of Proportionality in an Era of High Technology : Jack Beard; DOI:10.1093/oso/9780190915360.003.0009
4. Cyber National Security: Navigating Grey-Zone Challenges in and through Cyberspace, Gary P. Corn, DOI:10.1093/oso/9780190915360.003.0012
   https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-12
5. How should the US respond to ‘grey zone’ activity? By: Cal Pringle
   https://www.defensenews.com/global/the-americas/2019/07/12/how-should-the-us-respond-to-grey-zone-activity-here-are-three-options/
6. Competing in the Grey Zone- Russian Tactics and Western Responses by Stacie L. Pettyjohn, Becca Wasser
7. https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-6 Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare by Winston S. Williams and Christopher M. Ford ; Hybrid Warfare, Law, and the Fulda Gap by Aurel Sari
8. Mann Col Edward, USAF, 1994, Desert Storm: The First Information War? , Aerospace Power Journal - Winter 1994 (http://www.iwar.org.uk/iwar/resources/airchronicles/man1.htm) Accessed 30 Dec 2019
9. Fulghum David A. and Wall Robert, 2007, Israel Shows Electronic Prowess: Attack On Syria Shows Israel Is Master Of The High-Tech Battle, Aviation Week & Space Technology Nov 26, 2007 (http://aviationweek.com/awin/israel-shows-electronic-prowess) Accessed 30 Dec 2019
10. Katz Yaakov, 2010, And They Struck Them With Blindness: A Rare Glimpse Into Israel’s State-Of-The-Art Electronic Warfare Capabilities, (http://www.jpost.com/Magazine/Features/And-they-struck-them-with-blindness) Accessed 30 Dec 2019

11. Details of DRFM are discussed later in this paper

12. https://www.airforce-technology.com/features/feature1669/, Accessed 30 Dec 2019

13. Saurabh Tewari, Brigadier; Defending/Exploiting EM Spectrum Against/For Cyber Warfare; CENJOWS SYNODOS Paper: 2019.

14. https://info.publicintelligence.net/USArmy-CyberContest-2.pdf, Accessed 30 Dec 2019

15. http://mattcegelske.com/wp-content/uploads/2013/03/Information_Dominance_Roadmap_March_2013.pdf, Accessed 30 Dec 2019

16. http://idstch.com/home5/international-defence-security-and-technology/cyber/integrated-cyber-electronic-warfare-signals-intelligence-and-communications-operations-for-future-battlefield/, Accessed 30 Dec 2019

17. Ibid

18. https://www.army.mil/article/171596/army_announces_arcyber_as_an_ascc,Accessed 30 Dec 2019

19. Cole Harold T, Cdr, US Navy, 2014, Warfare In The Electromagnetic Spectrum And Cyberspace: United States Air Force Cyber/Electromagnetic Warfare Command Construct (http://www.au.af.mil/au/awc/awcgate /cst/bh_2014_cole.pdf) Accessed 30 Dec 2019

20. Sharma Deepak, 2010, Integrated Network Electronic Warfare: China's New Concept of Information Warfare, Journal of Defence Studies: Vol 4. No 2. April 2010, published by Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/jds/4_2_2010_ChinasNewConceptofInformationWarfare_dsharma) Accessed 30 Dec 2019.

21. Sharma Deepak, 2011, China's Cyber Warfare Capability and India's Concerns, Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/system/files/jds_5_2_dsharma.pdf) Accessed 30 Dec 2019.

22. Costello John, 2016, The Strategic Support Force: China's Information Warfare Service, China Brief, Volume: 16 Issue: 3, Jamestown Foundation (https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/) Accessed 30 Dec 2019.

23. https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/, Accessed 30 Dec 2019.

24. https://www.rand.org/pubs/research_reports/RR2058.html, Accessed 30 Dec 2019

25. Giles Keir, The Next Phase Of Russian Information Warfare, NATO Strategic Communications Centre of Excellence: p 13 (https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles) Accessed 30 Dec 2019.
26. Freedberg Sydney, 2015, Army Fights Culture Gap Between Cyber & Ops: Dolphin Speak, Breaking Defense, 10 November 2015,(http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/) Accessed 30 Dec 2019
27. Independent, 22 Feb 2017(http://www.independent.co.uk/news/world/europe/russia-military-information-warfare-hacking-allegations-a7594456.html) Accessed 30 Dec 2019.
28. Australian Government, Department of Defence CEWD Strategic Plan 2016-2021: p 21 (https://www.dst.defence.gov.au/sites/default/files/divisions/documents/CEWD_Strategic_Plan_2016-2021.pdf) Accessed 30 Dec 2019.
29. Ibid: p 22.
30. The Times of Israel, 16 Jun 2015 (https://www.timesofisrael.com/army-to-establish-unified-cyber-corps/) Accessed 30 Dec 19.
31. The Times of Israel, 14 May 2017 (https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/) Accessed 28 Dec 2019.
32. English translation available at https://www.belfercenter.org/sites/default/files/files/publication/ IDF%20doctrine%20translation%20-%20web%20final2.pdf,Accessed24 Dec 2019.
33. Ibid: p 9
34. Ibid: p 44.
35. https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/, Accessed 26 Dec 2019.
36. https://www.popsci.com/iran-anti-drone-rifle, Accessed 26 Dec 2019

Bibliography

1. Fitton, O. (2016). Cyber Operations and Grey Zones: Challenges for NATO. Connections, 15(2), 109-119. Retrieved from www.jstor.org/stable/26326443
2. Cyber National Security:Navigating Grey-Zone Challenges in and through Cyberspace; Gary P. Corn DOI:10.1093/oso/9780190915360.003.0012

https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-12.

3. How should the US respond to 'grey zone' activity? :Cal Pringlehttps://www.defensenews.com/global/the-americas/2019/07/12/how-should-the-us-respond-to-grey-zone-activity-here-are-three-options/.
4. https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final2-web.pdf Bryan Clark , Mark Gunzinger& Jesse Sloman; Winning in Grey Zone using EM Warfare to Regain Escalation Dominance, CSBA Pub
5. Competing in the Grey Zone- Russian Tactics and Western Responses by Stacie L. Pettyjohn, Becca Wasser.
6. https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-6 Complex Battlespaces:The Law of Armed Conflict and the Dynamics of Modern Warfare ,Winston S. Williams and Christopher M. Ford.
7. https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-9 The Principle of Proportionality in an Era of High Technology; Jack Beard; DOI:10.1093/oso/9780190915360.003.0009.
8. https://www.oxfordscholarship.com/view/10.1093/oso/9780190915360.001.0001/oso-9780190915360-chapter-11

   New Technologies and the Interplay between Certainty and Reasonableness; Laurie Blank; DOI:10.1093/oso/9780190915360.003.0011

8. Saurabh Tewari, Brigadier; Defending/Exploiting EM Spectrum Against/For Cyber Warfare; CENJOWS SYNODOS Paper: 2019.

GREY ZONE THREATS AND COUNTER STRATEGIES

Lt Gen AB Shivane, PVSM, AVSM,VSM (Retd)*

Changing Character of Warfare

War has been a permanent preoccupation of mankind to settle all disputes, in over six thousand years of recorded history. Confrontation, conflict, hostility and wars have historically not only been intrinsic but also logical to resolve differences in ideologies, religious faiths and societal values or to acquire a greater share of resources / territory or prestige and power. With the emergence of sovereign nation states, the conflicts transformed into increasingly inter-state all out wars, focused on territorial and resource expansion. However, in the last few decades, the technology enabled colossal destructive power of conventional and nuclear capabilities, have resulted in states and non-state groups shifting to sub-conventional irregular means or proxies to achieve their political objectives, with attendant deniability and ambiguity, referred as Grey Zones. Further, nuclear deterrence and globalisation created interdependencies, impacting high economic cost of war between nation states, changed the complexion of “all out wars” unviable to justify, prosecute or sustain, down to the “Grey Zone”. The more lucrative option for pursuing strategic interests below the threshold of traditional armed conflict, thus found favour in Grey Zone warfare with hybrid tactics. Some describe conflict in the Grey Zone as “competitive interactions among and within states and non-state actors that fall between the traditional ‘war’ and ‘peace’ duality”. This in the Indian context is often referred as “No War No Peace “or NWNP state.

Conceptual Contours of Grey Zone Conflict

The concept of “Grey Zone”, conflict has generated much debate and controversy amongst strategic studies communities and uniformed fraternity. It is seemingly straight forward but fraught with complexities,

contradictions, and ironies. Grey zone has indeed found innumerable dissimilar definitions, but with similar strategic security connotations. It has also been associated with 'old wine in a new bottle' and the fashionable unfolding of new terminologies in warfare scripting. Nevertheless, essentially grey zone is an operational space between peace and war, occurring when actors purposefully use coercive actions to change the status quo below a threshold, to achieve desired strategic outcomes. Such activities take advantage of strategic ambiguity and deniability to achieve gradual gains and political security objectives. The fundamental operational aspects of time, space, force and information of this ambiguous grey zone however remain unambiguous and discerning. Grey Zones activities thus can be characterized by lack of attributability and attendant deniability to deflect responses; gradual unfolding over time rather than a bold military actions that could be easier to identify and respond; use of nonmilitary tools ensuring these elements remain below the threshold to justify a military response; legal,moral, political and historic justifications for supporting grey zones where ambiguity pointers are compromised; target specific political, social, economic, ideological, ethnic fault lines and vulnerabilities of target countries and challenging and undermining international norms or laws exploiting ambiguity of identity; and lastly where the lines between military, economic, diplomatic, intelligence and criminal means of aggression become increasingly blurred. Thus, Grey Zone approaches by nations and non-state players have donned varying names like 'proxy war', NWNP, political war, trade war, invisible wars, shadow wars etc. The basic underlying fact being that grey zone approaches are synonymous to revisionist outlook disguised to varying degrees, yet aim to alter territories, regimes, ideologies or any other established system, without exposing the practitioner to the responses and perils that escalation beyond threshold might bring. The means applied could be unconventional coercive tactics, from disruptive cyber-attacks, to propaganda and political warfare, to destabilizing social media influence, to economic coercion and sabotage, to sponsorship of armed proxy actors and terrorism, to incremental aggression.

A distinction also needs to be made between hybrid warfare and grey zone conflicts to better understand the continuum of states engaged in grey zone conflicts. Essentially, hybrid warfare emphasizes the tactical level, while grey zone conflicts, incorporate a long-term strategic

dimension to achieve political objectives. The revisionist element in grey-zone conflict differentiates it from hybrid warfare. Thus, hybrid tactics can be considered as a tactical subset of grey-zone conflict.

Expanding Envelope of Grey Zone Conflict

Numerous examples of Grey Zone conflicts existed, exist and will continue to dominate the 'clash of wills' in the contemporary world. Grey Zone conflicts are thus becoming the new normal with the recent examples as the Russia's use of armed proxies to destabilize and dismember Ukraine with unacknowledged aggression, the growth of ISIL in the Levant threatening global energy markets and regional stability, the Boko-Harim terror incursion into West Africa, the Houthi rebellion in Yemen and Iran using subversion and proxy warfare to destabilize adversaries and shift the balance of power in the region.

India too has been the target and victim of the grey zone warfare capabilities of Pakistan and China. China's preferred instrument against India is psychological warfare with coercive tactics. China has extensively used the information warfare, media, psychological and legal warfare to subdue Indian power calculus in South Asia and the Indian Ocean Region. The Chinese strategy is a surreptitious long term ploy professing peace and tranquillity but periodically disturbing status quo and unleashing political warfare, designed to subdue India's growth and predominance without involving non-state actors or kinetic attacks. Similarly, the philosophy of unrestricted war followed by China is omni-directional and has the potential of application in the cyber, information, and economic spheres. China is also using grey zone as part of a campaign of incremental expansionism in the South China Sea. Conversely, Pakistan has mastered the art of employment of regulars and irregulars along with non-state actors and the conflict in Jammu and Kashmir is a manifestation of this capability. The most satanic demonstration of grey-zone operations in South Asia, however, came in the form of the 26 November 2008 attack on Mumbai, aided and abetted by Pakistan but with unwavering deniability. Thus, India must acknowledge that grey zone wars and grey zone collisions undermining national security are here to stay and will require greater understanding and a comprehensive national power response. Further, grey zone warfare is not only a tool of the weaker state like Pakistan but also of a

strong state like China. Therefore, manifestation of collusive grey zones by Pakistan and China are a reality and no more a myth. China cannot also fathom India's rise and global recognition and as such encourages Pakistan's pugnacity against India to dominate the geostrategic and economic space. Thus, distraction to tackle the weak must not lose focus of the bigger threat, which if tackled with a long term strategic security perspective would automatically subdue the weaker threat and the collusive bondage. Indeed Pak- China tango will continue to be on the front stage of global geopolitics while the Chinese checker will continue to aspire to keep India strategically contained. In turn India's Chanakya Niti must checkmate the Chinese strategy of Sun Tzu. A balanced comprehensive strategic approach to countering grey zone aggression is thus mandated.

Grey Zone Conflict and Notion of Victory

In Grey Zone conflicts, defeat of the enemy may not be attainable nor is the word "victory" applicable to the conflict. Thus, notion of victory, is as grey as the conflict or its grey zone actors, with victory or defeat being replaced by "perceived success", based on induced perception and clouded by information warfare. There may well be no victor or vanquished with either side claiming success. Therefore, success of a nation's grand strategy must be measured in terms of distinguishing outcomes as 'better' or 'worse' as events unfold. Strategic objectives being achieved depend on the full government response encompassing diplomatic, cyber, informational, economic, political, legal, asymmetric, and military to achieve appropriate goals. The defining principle of dealing with grey zone conflicts is thus 'unified effort', 'borderless boundaries' and dominating the 'perception space' at strategic level. Success in such zones is dependent on exercising strategic patience, thus the need to envision, institutionalize long-term strategy and devise innovative means of deterring and defeating grey zone actors. The means could entail actions to isolate, controvert or renounce them from the human terrain and proactively disrobe their surreptitious cloak. Policy of retribution or punitive deterrence to make the grey zone conflict cost prohibitive acts as deterrence, but the levers of escalation must be managed to one's advantage. Thus, modern deterrence must also focus on deterrence by sustained resilience with a proactive disposition. Success in building

resilience depends on the ability to forecast a desired end-state that prioritizes long-term political, security and economic goals.

Grey Zone Deterrence Strategies in the Indian Context

India should not become a victim of grey zone war or casualty, because of its own neglect. There is a need to introspect, analyse and formulate strategies to have an effective mechanism to deal with it. The basic operational approach to gaining ascendancy in grey zone is no different than that of conventional warfare in terms of "deny, dissuade /deter, mitigate and defeat", albeit, proactively deny space to grey zone actors, deter / dissuade grey zone adventurism, mitigate by building resilience and comprehensive response, and defeat the threat with a whole of nation approach. Grey zone deterrence must also lay equal emphasis as military dissuasion, on shaping strategic environment through political, diplomatic and informational outcomes against an adversary and minimise the 'social space' in which the grey zone actors prevail. Further, Grey zone threats are not all created alike, and neither are their responses. Some grey zone threats require immediate action like in the case of Pakistan, while others like China may require long-term persistent dissuasion through political, diplomatic, economic, cyber, informational, political, legal messaging and developing all-encompassing credible military capabilities for deterrence. An often overlooked strategic underpinning in grey zone deterrence is that the levers of making grey zone warfare cost prohibitive for an adversary lies in the development of asymmetric conventional response capability messaging "Behave or Else….". However, any strategy for responding to grey zone aggression must balance and firmly control the levers of escalation including military, diplomatic, and economic aspects with the reality that, to be effective, countering grey zone threats demands some degree of risk tolerance and grey zone responses. It is also pertinent to realise that grey zone warfare are a symptom of broader regional ambitions and competing aspirations and cannot be addressed outside that context. Never the less, in a globalised world where international opinion matters, exposing grey zone actors must be an inherent part of coercive deterrence diplomacy, while being prepared for "go-it-alone" responses when essential. Thus the strategic aim and intentions of grey zone adversaries must be lucidly interpreted and be central to focused deterrence strategies. This

would energise a proactive rather than a reactive response strategy to coercive threats and deter future manifestations. Confronting grey zone challenges requires both embracing and dispelling ambiguity. Thus grey zone threat scenario building and response matrix must be part of envisioning future grey zone threats and developing tools and approaches to respond effectively.

A critical component of grey zone deterrence strategy is orientation and an organisation framework to meet grey zone threats, rather than just resource building. A well-structured organisation for a comprehensive whole of government proactive approach responding in all dimensions namely, military, diplomatic, informational, and economic is an imperative. Thus at the national level a balanced strong policy and grey zone deterrence coordination mechanism, that can allow coherent and effective responses must be institutionalised. The recently raised Department of Military Affairs must well be empowered to be an intrinsic part of this response strategy structure. This structure must focus on developing grey zone deterrence capacities and communicate the same with demonstrated political will and desired strategic response capabilities. The focus of this structural mechanism must not only be to mitigate grey zone threats but gain strategic advantage by leveraging all tools of statecraft while controlling escalation matrix. A key to developing this structure is development of human capital to execute grey zone deterrence both at the government and military level.

Another core element of this deterrence is a finely balanced time critical punitive response capability to any grey zone provocation. In particular intelligence fused surgical strikes, precision targeting and information operations at the military level accompanied by coercive diplomatic, political and economic policy must be inherent to the strategy of grey zone deterrence. Status Quo or strategic inertia termed as strategic restraint or risk aversion will not only be counterproductive, but in fact expand the space for grey zone aggression. A punitive deterrence capability must also balance a proactive strategy for exploitation of fault lines and weaknesses of grey zone adversary to gain moral, phycological and physical ascendancy, as well as a retributory response strategy to mitigate any threat that may so manifest. The new normal must exhibit certainty of response in varying shades, even in the fog

of adversary's traditional deniability with uncertainty of intensity and medium, irrespective of the strategic restraints. It must demonstrate the nations resolve, strong political will and multi domain capability for a comprehensive punitive response to grey zone national security threats.

Conclusion

Grey zone threats are a reality of contemporary warfare which are only likely to expand both in manifestation and effect in the future. India has been and likely to be in the foreseeable future a target for such grey zone aggression. Thus there is a need to introspect, envision and formulate grey zone deterrence strategies and structures to deny, deter, mitigate and defeat grey zone threats with a whole of nation approach.

***Lt Gen AB Shivane, PVSM, AVSM,VSM (Retd)** is a former DG Mech Forces

GREY ZONE WARFARE: EMPLOYING PROXY FORCES FOR ATTAINING POLITICAL OBJECTIVES

Lt Gen Syed Ata Hasnain, PVSM, UYSM, AVSM, SM, VSM (Retd)*

General

Before diving into the world of proxies and the significance they hold in current and future wars it may be worthwhile to outline an understanding of 'grey zone' and its differentiation from 'hybrid war'. The role of proxy forces in these domains is only going to increase as the world realizes the futility of all out conventional war and exploits the enormous utility of emerging technologies in determining intensity of warfare to meet varying objectives. The Cold War itself witnessed the sponsoring of states for exercising indirect influence over a region. That may not fit the classic understanding of proxy war but as outlined in this paper proxy nations and their worth will only increase the effectiveness of proxy wars as technologies take a leap into unchartered territories, particularly the world of finance, information and influence.

Concept of Proxy Forces

The mention of 'proxy forces' immediately conjures in the mind perception of three conflict domains of recent years, two of them ongoing. The first really effective employment of physical proxies in modern times was during the war in Afghanistan in the period 1980-89. The Soviet Union had invaded Afghanistan at the end of 1979 to supposedly guard its soft underbelly and undertake in the next step a push to the Indian Ocean. Without the homeland being directly threatened the US chose to resist the Soviets indirectly through the employment of trans-national proxies, sponsored and financed by Saudi Arabia, equipped by the US itself and provided leadership in the field by groups of Afghans directed by Pakistan's notorious intelligence service, the ISI. The concept was a

success but it was far too close to conventional warfare by non-state proxies directed by sponsors. The idea's second coming was in 1990 when Pakistan unleashed a similar campaign in Kashmir. It demonstrated Ziaul Haq's doctrine of a thousand cuts to bleed India with retributive intent; the campaign continues to the day, albeit largely emasculated but with potential of revival. The third and also an ongoing commitment has been the extensive use of proxies by Iran to spread its dragnet in West Asia to pursue its twofold intent of resisting US coercion and upending a Saudi sponsored campaign to enhance influence of its religious ideology. All three examples above have employed variable shades of violence as part of the concept. However, the limited employment of violence has been aided by progressive use of emerging technologies of the times, although violence and even part attributability continued to form a part of it.

Move beyond Conventional Conflicts

The last thirty years have also witnessed the receding of the employment of conventional domain of war fighting with increasing usage of limited and elongated campaigns of hybrid conflict. This has resulted from the onset and the availability of different shades of coercion beyond just the use of unbridled violence. The quickest off the blocks was China just after Gulf War I in 1990. The People's Liberation Army (PLA) yet at a lower priority in the field of China's four modernizations, utilized this time to deeply study the influence of the information domain which contributed to the US and Allied success in 1990. From there emerged its first study and doctrine – 'War under Informationised Conditions', leading finally in 2003 to the doctrine of 'Three Warfares' which consists of public opinion warfare, psychological warfare, and legal warfare. Developments in the field of war technologies in the second half of 19th Century and most of 20th Century focused upon the physical domain of destruction. On the other hand the period since 1990 has exploited information technology to ratchet up the effectiveness and accuracy of war fighting technologies but more than that, concentrated upon information and influence to promote non-physical foreign intervention as domains of warfare.

Grey Zone and the New Spectrum of Conflict

One of the major impacts of the above developments has been the intense crowding of the spectrum of conflict with non-traditional domains

entering it with overlaps galore. Information technology has opened vistas above imagination and given capability to nations to employ proxies beyond just the domain of the common understanding of proxy war involving just limited physical coercion through terror acts. For a broad understanding of some fresh domains in the conflict spectrum we could include cyber, financial networks triggering political and financial scams, fake currency, electronic subversion, clandestine foreign influence in internal affairs, criminal acts, electoral manipulation and economic insider subversion for unethical advantage. This is just the tip of the iceberg with rapidly emerging new domains enhancing the scope. This analogy helps understand Grey Zone Warfare which as per one definition 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. The 'zone' essentially represents an operating environment in which aggressors use ambiguity and leverage non-attribution to achieve strategic objectives while limiting counteractions by other nation states". The catchwords remain 'ambiguity', 'threshold' and 'non attribution'. All three combine to make this complex enough to create a response dilemma for the target adversary due to the situation being in the grey zone.

On the other hand hybrid warfare is an ill-defined notion in conflict studies. It refers to the use of unconventional methods as part of a multi-domain war fighting approach. These methods aim to disrupt and disable an opponent's actions without engaging in open hostilities. There is similarity between grey zone and hybrid warfare but yet subtle differences. It is best to consider grey zone warfare as the larger umbrella concept of employing multiple domains to achieve ends which hybrid warfare alone cannot achieve. Although not explicitly stated in research outputs I believe that hybrid warfare exists in state of higher animosity with the crossing of certain benchmarks in the standoff, well short of conventional military engagements but yet willing to use coercion as a tool. Grey zone warfare alludes to a more layered situation, a terrain where conflict potential exists but is held back by the advantages of other engagement; yet the grounds are constantly under preparation through non-military intervention, influence operations to subvert civil society, having greater control over and achieving dominance in financial

networks to effect manipulation, creating dissension to prevent social and political consensus and thus compromising legislation and electoral outcomes through possession of the capability to unleash criminal networks in the cyber domain and areas such as fake currency. It has the characteristics of hybrid warfare, in that it has hybridity built in it.

Proxy Forces in West Asia

The employment of proxies for political objectives need not any longer conjure only perceptions of ragamuffin, ideologically oriented non state actors ready to be employed as terrorists. Full states can act as proxies and no better example than that which exists in the long standing US-Iran standoff. The US is aware of its limitations to coerce Iran into a desirable strategic behavior and its interests lie in preventing the spread of Iran's influence in West Asia. Regime change being one of its other political objectives, the US has therefore to work both inside Iran and outside in the region to isolate it in every conceivable way. Proxy states forming part of its strategy include Israel, Jordan, Saudi Arabia and the Gulf kingdoms with investment in Iraq also remaining for future scenarios. Retention of limited military deployment in its bases in most of these countries provides a sense of psychological security of the hosts besides facilitation of surge if necessitated. The US politically exploits pan Arab Sunni identity, bolstering it against Iranian Shia influence and uses its economic muscle to keep its partners stable. Its physical presence gives opportunity to continue surveillance and cultivate political influence both within the proxy states and elements inside Iran. War is unlikely but the grey zone exists where potential for war remains contingent upon the nature of triggers. Proxy powers ensure stability and counter balance Iran's capability. While the US may not directly meet all its political objectives the influence it bears and the potential it projects limits Iran's ambitions. Ambiguity, uncertainty, threshold and non attributability all form a part of the proxy strategy in the grey zone, awaiting potential success.

The grey zone need not witness just one sided efforts and may witness mutual use of proxies, albeit of a different variety. The US strategy depends on full regional states through the political, cultural and economic domains, along with coercive acts such as assassination,

the targeting of Iran's Quds Force Commander being an example. Iran however has a push back strategy of its own. It follows classic proxy strategy employing limited violence, selecting targets with an intended attempt to stay below the threshold of terror acts. However, this is not always achieved especially in relation to Israel. Its political strategic intent remains the spread of influence and is aided in this by the existence of ideologically similar minority populations and in one case (Iraq) a majority. Retention of strategic autonomy is its other intent. It is the threat of use of sponsored violence which continues to influence the strategic behavior of its adversaries. The development of offensive cyber capability is the other domain in waiting which assists in the achievement of its intent. The promotion of the Bashar Assad regime in Syria and lately the Hezbollah controlled government in Lebanon are also examples of full nation states acting as proxies. On balance, it is two widely varying strategies in the use of proxies in a grey zone which maintains the balance with situations sometimes veering towards escalation as we have recently witnessed. Escalation control is not guaranteed but responses are per force kept within limits with deterrence playing its role.

Russia's Experiments

Russia is the other power which has demonstrated the usage of hybrid war under grey zone conditions of ambiguity, threshold and non attributability. It follows different models in different regions and against different adversaries. As per Mark Tarallo, "its first goal is to reestablish influence over former Soviet countries; the second is to reclaim its global status as a great power; and the third is to take on the role of a key regional power broker, which would allow it to increase its military and political sway over nations around the world". Against the US mainland it uses political fifth columnists as proxies with the assistance of information and influence operations. The intent goes as far as intervention in the electoral process to secure influence in high places of decision making. Emerging technologies in the world of innovative financial networks provide anonymity which can help in undetected influence operations. The use of diaspora too may be resorted to. Another example of Russia pursuing its aims is in the Baltics where it is exploiting the discontent simmering within the already large and growing community of ethno-linguistic Russians who live there. This diaspora has the potential to

act as influence spreading proxies who use social media to spread information and disinformation. Political objectives are clear in a region uncomfortably close to Russian borders. It must be won back to the Russian fold from the dangerous influence of NATO and the European Union whose members the three states are.

Proxy Forces in the Indian Subcontinent

Perhaps an example of classic vulnerability to hybrid war under grey zone conditions exists in the Indian subcontinent. All the nations are prone to it while India at the centre bears a special vulnerability directly and indirectly through its neighbors. The Chinese model perhaps comes closest to classic grey zone strategy. With India its perceived main rival in Asia, China's political objectives are clear. First is to limit Indian comprehensive national power through the creation of security vulnerability via its neighborhood. It's a model much like the US uses in West Asia by cultivating influence over Iran's neighbours, and tethering their strategic interests to its own to prevent the expansion of Iran's influence. China constantly strategizes to cultivate and influence India's neighbors and indirectly target India. Economic assistance helps in political cultivation as witnessed in Sri Lanka and Maldives at different times. The second political objective is to create dissension in Indian border states in relation to their linkages with peripheral nations across the borders. The third political objective is to prevent India rising to its true potential by imposing on it security constraints which impact its economy, internal unity and diplomatic choices. China resorted to use of physical proxies many years ago particularly in the North Eastern states to trap India in an internal security spiral. Its assistance to separatist elements has never been with intent of secession of these states; it's the turbulence which delivers far more than achievement of secession. The Red Corridor of India where a Communist oriented insurgency continues, albeit at much lower level today has some limited linkages to China. The connect with Maoism, an ideology which China itself has rejected, helps in promotion of the grey zone; restiveness in the heart of India can only aid China's politico-strategic intent. Overall China is least likely to seek war against India with whom it has an advantageous economic relationship as its intent is met by adhering to the strategy of grey zone warfare. What is evident is that in the future there will be far greater

employment of information warfare, political manipulation through proxy political maneuvering, economic warfare and cultivation of influence among India's neighbors. India's inability to take along its near abroad region could hurt it and make it more far more vulnerable especially as it struggles with the necessity of networking these nations closer in the economic domain. These networks can have reverse negative effect in the social and political domains.

Pakistan's Use of Proxy Forces in the Grey Zone

The biggest vulnerability in the politico-strategic domain that India faces is the existence of numerous demographic fault lines. This lies in the domains of regionalism, linguistics, ethnicity, caste and faith. Despite its stupendous achievement in weaving its vast diversities into a national fabric with full and well recognized democratic credentials India has witnessed slippages in standards of its politics. Political consensus especially on national security issues is elusive making the nation vulnerable to the exploitation of cleavages in society. A traditional adversary is Pakistan which being militarily weaker finds these cleavages an invitation for exploitation. Pakistan has a territorial issue with India over Kashmir but besides this its political objectives remain the prevention of India rising to its true potential, the hyphenation of Pakistan with India through the conflict domain and creation of disunity in society. It uses the hybrid conflict route and is fast stepping into the realm of grey zone warfare by the expansion of its strategy with the key terms – manipulation, disorder, ambiguity, threshold and denial to achieve non-attributability, as essential elements of the strategy.

The experience that Pakistan and its various strategic organisations gained in the Eighties in Afghanistan has been progressively used against India. The core centre of concentration is Jammu & Kashmir (J&K) with peripheral activity in other vulnerable regions such as Assam and other North Eastern states, Central India, and the Southern region. Proxy forces comprise locally recruited terrorists, infiltrated Pakistani terrorists, sleeper agents, over ground workers and fifth columnists. This is avidly supported by the Inter Services Public Relations Wing (ISPR) in recent years through information and disinformation facilitated by the spread of the tentacles of social media through the internet. Information boundaries no longer exist in the era of Twitter, Facebook and Whatsapp.

For many years it has also created financial and criminal networks which feed the campaign. The information domain has facilitated the potential of political manipulation through sleazy back channel contacts with money playing a major role. Ideological radicalization although denied by many within India, does play a contributory role. This was a part of the Ziaul Haq doctrine which helped change the ideological orientation of some within Kashmir; the intent being the creation of an ideology opposed to India's secular and tolerant culture which could then be tethered to Pakistani interests at will.

Target states such as India usually prefer the status quo and remain in denial of the enormity of threats when they are subjected to grey zone warfare. This is what happened with relation to J&K in 1987-90 when the buildup of Pakistani intervention was in progress. The irony in India's case was the weakness of its strategic culture. It was then being targeted by hybrid warfare without any realization of it and the response was only in the field of counter terror while hybrid warfare needs an 'all of government' approach. In today's world, which has moved on to grey zone warfare, the complexity enhances even more. Plain military and police response will not make a dent as the domains extend into the civilian realm; legal, ideological, financial, information, political manipulation and several other domains which go into making this environment, only add to ambiguity. It creates severe challenges in response without political consensus and consensus is something India has been progressively losing in its political and social environment. This works ideally for adversaries to maintain momentum in their campaign as the target nation ties down its effectiveness. Progressively Pakistan's role in areas outside Jammu & Kashmir is likely to expand as polarization of Indian society increases and its search for new proxies along with the phenomenon of information and influence operations, is going to make for challenging times for India's intelligence and security organisations. Wading through the grey zone is not going to be easy.

Pakistan's success in Jammu & Kashmir till recent times appeared considerable. However, since 2016 understanding of Pakistan's strategy and the inadequacy of its own response has been better realized by Indian functionaries. Such campaigns by an adversary are dependent upon eco-systems created to sustain continuity; these systems have sub

components each of which requires neutralization. Since 2017 India's National Investigation Agency (NIA) has been successful in dismantling some of the networks which ran finances and executed out of proportion political influence through the media. The separatist leadership has also been neutralized far more than before but the detention of mainstream political leaders and the elongated lockdown of the mobile internet have fetched international criticism which can only grow and needs to be better handled after the initial success which had been gained. The lesson is that diplomacy and external influence operations by the target state have to remain in continuum to ensure moral ascendancy in an environment in which proxies promote victimhood as an instrument.

Conclusion

It is clear that the Grey Zone concept is yet in its infancy and many more domains will be added to its own spectrum. It's a growing concept which will continue to exploit emerging technologies and the systems that are created in their wake. The concept of only physical proxies may be passé as fresh methods of manipulation and influence are developed. Inside jobs as part of proxy campaigns will multiply. Target nations will have to ensure that their diversities are not laid open to exploitation. Better political management and consensus along with strengthening of institutions and systems that run them will have to receive much more attention. Yet the age old war concept of initiative being retained by those who undertake the offensive will continue as before, leaving target nations and societies vulnerable unless they can correctly identify and recognize these vulnerabilities and proactively overcome them.

***Lt Gen Syed Ata Hasnain, PVSM, UYSM, AVSM, SM, VSM (Retd),** is a former GOC of India's 21 and the Srinagar based 15 Corps, with much experience in the handling of proxy operations. He is currently the Chancellor of the Central University of Kashmir

GREY ZONE WARFARE: VICTORY WITHOUT FIGHTING

Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)*

" Hence to fight and conquer in all your battles is not supremer excellence: supreme excellence consists in breaking the enemy's resistance without fighting"

- SUN TZU on the "Art Of WAR" (III.2)

On October 18, 2014, Prime Minister Narendra Modi in the Combined Commanders' Conference said, "Beyond the immediate, we are facing a future where security challenges will be less predictable; situations [1]will evolve and change swiftly; and, technological changes will make responses more difficult to keep pace with. The threats may be known, but the enemy may be invisible. Domination of cyberspace will become increasingly important. Control of space may become as critical as that of land, air and sea. Full scale wars may become rare, but force will remain an instrument of deterrence and influencing behaviour, and the duration of conflicts will be shorter." This clear and categorical direction emanating from the Prime Minister himself, is indicative of future threats and challenges to national security. The security challenges for the nation can no longer be defined and definite, as these are likely to be in the Grey Zone, conducted in many battle spaces by multiple means driven by a collective ideology, plausibly without any direct attribution and without any overt physical military application of combat power ab-initio.

In essence Grey Zone warfare is as old as warfare itself, however, in an interconnected, networked digital world, a world with vanishing borders but with conflicting interests and competition for resources

1 http://www.narendramodi.in/pms-address-at-the-combined-commanders-conference

among people, regions, religions, civilisations and nation states, new cost effective methods of waging wars are emerging. War is never an option but the proverbial last resort. Nations go to war to impose their will on the adversaries, the mightier nations historically have succeeded in achieving victory through wars. New age technologies coupled with the vulnerabilities of mega nations have given rise to asymmetric capabilities to smaller nations and ideology based groups to wage wars to either propagate or impose their will on other nations and society. The world is changing at a pace not seen in history earlier, as is the ends, ways and means of warfare.

The proposition of this paper is the idea of winning without fighting, though an age old concept it has seldom been practiced with success. There have been 16 transitions of world power in the last five centuries, of these eleven have been violent and only five peaceful. As the world anticipates another transition of power in the near to mid term with China challenging the US hegemony, it is imperative to discuss and study the shape and contours of emerging challenges.

Sun Tzu's Art of War, a 2000-year old Chinese book of military strategy extols "those who render others' armies helpless without fighting" saying "rather than overcoming his enemies on the battlefield, the superior general infiltrates their ranks, uncovers their secrets, fosters discontent and disharmony and destroys their alliances, thus eroding their willingness to fight". In present day context 'winning without fighting' will also imply fighting in the Grey Zone and exploiting new age technologies to change the behavior of nations and societies, this could in a larger sense also be imposing your will on the adversary by employing nonviolent methods. Mahatma Gandhi the greatest proponent of non violence succeeded in defeating the might of the British Empire forcing them to quit India. Gandhi can rightly be called the father of non violent warfare or Grey Zone warfare in its ultimate sense proving to the world the concept of " Winning without Fighting".

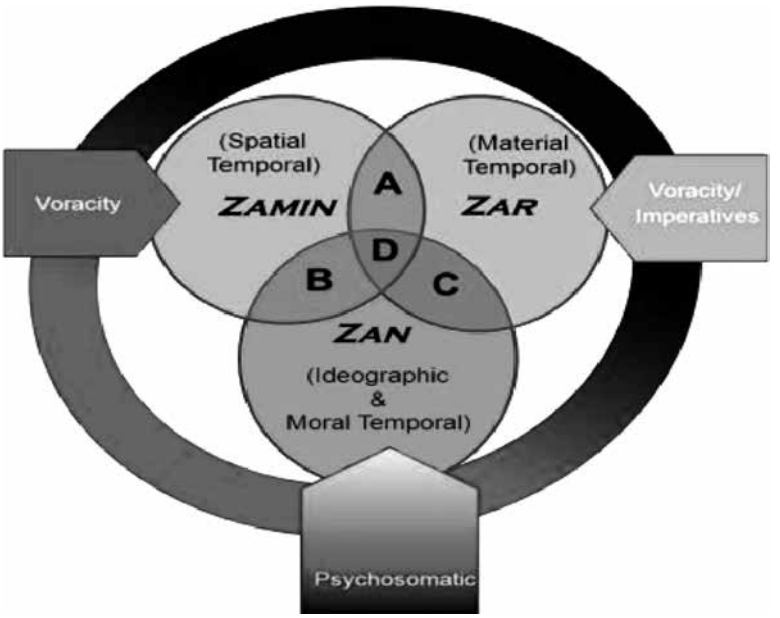
The notion of victory is a study in itself. Mohammad Iftikhar Zaidi in his thesis The Conduct of War and the Notion of Victory for Cranfield University argues that a bivariate approach is that triangulates desired ends with the opposing notions of success and perception of defeat. The theory presented encapsulates traditional precepts, adds new ones

and simplifies the complexities that have come to surround victory in contemporary times. Offered are some valuable ingredients to flavour any strategic recipe, not just war and conflict. The eternal challenge of calibrating means and ends needs more systematic awareness of functional and dominant domains of victory which, it is argued, is possible through application of simple principles. The theory potentially allows for a more focused, proportionate, efficient and productive use of power. It is hoped that strategists and analysts alike, would find here new concepts and tools for use in praxis, perspective planning and retrospective analyses. [2]

Grey Zone warfare has been discussed and deliberated upon in a number of articles by well recognised military experts in this very journal, and hence the focus is on 'Winning without Fighting". What's the notion of victory? Clausewitz described military victory as a condition where the enemy's ability to enter battle, resist or resume hostilities is destroyed. The notion summarises the paradigms of success that preceded Clausewitz and survived through much of the 20th century. Is such a doctrine of victory still valid? The short answer is NO; and yet, despite increasingly paradoxical outcomes, military planners, strategists and statesmen continually seek answers for their failures in variously perceived causative influences. Few question the validity of the Clausewitzian doctrine of victory that drove their initiatives. The rapid transformation in society and international culture has brought with it changes in geo-political and geo-economic relationships as well as warfare. While the traditional linkages between war and politics remain, the mechanisms driving these have altered. In less than absolute wars,' it is the wider bargain and the stakes in that bargain that make the enemy do our will' and not purely the opposition's inability to enter battle, resist or resume hostilities.[3] Zar, Zamin, Zan have been the drivers for conflicts over the ages and the basic causative factors are unlikely to change ever both through time and civilizations. This aspect has been diagrammatically explained by Mohammad I. Zaidi Political Science Published 2010.

2 The conduct of war and the notion of victory : a theory and definition of victory Mohammad I. Zaidi Political Science Published 2010

3 Ibid.



David Carment a CGAI Fellow and Dani Belo in October 2018 paper for CGAI write that today's geopolitical conflicts reflect a desire by some states to gradually, but fundamentally, revise the regional or global system of alliances and international norms to a degree not even seen during the Cold War. This process of conflict-induced change is known as grey-zone conflict, in which states conduct operations that only occasionally pass the threshold of war. Grey-zone conflict refers to those post-Cold War conflicts – not always violent – which are prolonged and frequently characterized by an ambiguous point of victory[4] (Carment, Nikolko and Belo, 2018). The paper further delineates two distinct phenomena in international affairs – hybrid warfare, which emphasizes the tactical level and grey-zone conflicts, which incorporates a long-term strategic dimension into international disputes. They argue that hybrid warfare can be a tactical subset of grey-zone conflict deployed under certain conditions and in varying degrees. One reason for this dual approach is the circumvention of, and asymmetric adherence to, international law. Simply put, international legal structures

4 War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare Carment, Nikolko and Belo, 2018.

act as restraints on what democratic states can do in the international arena. Hybridism offers a way out to avoid exploitation by states that do not uphold such laws. Permissive and advantageous conditions are created for non-democratic states to conduct operations against their democratic adversaries. Highly centralized, and thus procedurally flexible, states such as Russia and China can use propaganda, domestic legal structures, economic pressure and support for non-state proxies more readily, compared to democracies. This relatively unregulated environment enables authoritarian states to normalize and internalize new practices for engagement against opponents. In contrast, there are clear limits to what democratic states can do with hybrid warfare.[5]

The key question for states, rogue states and non state actors is how to win without fighting. The need to impose the will and change behaviour of adversaries remains the essence of conflicts and wars. In an earlier paper for Synergy Journal of CENJOWS the author has explained the changing nature of warfare, propounding that the nature of war has been and will remain an act of imposing one's' will on the adversary. However, the character of war i.e how future wars will be waged and fought has undergone a change due to numerous geo-political and socio-economic factors, technological advancements and military innovations. Future conflicts are likely to involve states or a state-sponsored actor as one of the participants of the conflict. States will also predominantly determine the spectrum, location and duration of conflicts. The last major driver of change that has had the foremost impact on character of war and the future operating environment is technology. Technological developments including artificial intelligence (AI), machine learning, data analytics, additive manufacturing, robotics, unmanned weapon systems, nanotechnology, quantum computing, brain-computer interface, bio-technology etc are rapidly changing the way future wars will be fought. Arguably the most important potential technology of all is AI. AI would overcome the four challenges of data processing – scale, speed, complexity, and endurance – necessary to analyze the increasing data from connected sensors. This will enable unmanned systems to have enhanced mission duration & effectiveness, reduce operating costs and risks to military personnel. Advancement in AI will also enable development of other complex technologies

5 Ibid.

including autonomous systems, additive manufacturing, biotechnology, manufacture of advanced materials etc. LInear wars as known will continue to be an important subset of warfare, however the very nature of warfare has changed and continues to change rapidly as new age technologies provide hitherto unknown tools and cost effective ways to wage wars both directly and indirectly.

Future threats also emanate from both known and covert adversaries in the form of changing the behaviour of a society, the values and beliefs. This could be done by simple means of exploiting the social media platforms in an innocuous and innocent looking long term campaign. Information warfare today is the most critical form of warfare as witnessed in the recent 3rd January 2020, US drone strike in the assassination of the Iranian General Soleimani. Closer home the Indian Air Force executed effective precision strikes at JeM terrorist training camp at Jabba Top, Balakot in Khyber Pakhtunkhwa in Pakistan. Though the strikes were perfectly executed but a well laid out information campaign by Pakistan DGISPR won the day and war as all Pakistanis were made to believe that they won the skirmish defeating the might of Indian military. Perceptions matter more than facts. New age warfare is equally a war of narratives, where fires are brought to bear not only in the kinetic domain but also in the virtual domain. Today's world is an interconnected networked world with billions having easy and instant access to numerous apps feeding their narratives and perceptions of events and happenings around the world. Whether you are a strategist or a terrorist, if you don't understand how to deploy the power of social media effectively you may win the odd battle but you will lose a twenty-first century war.

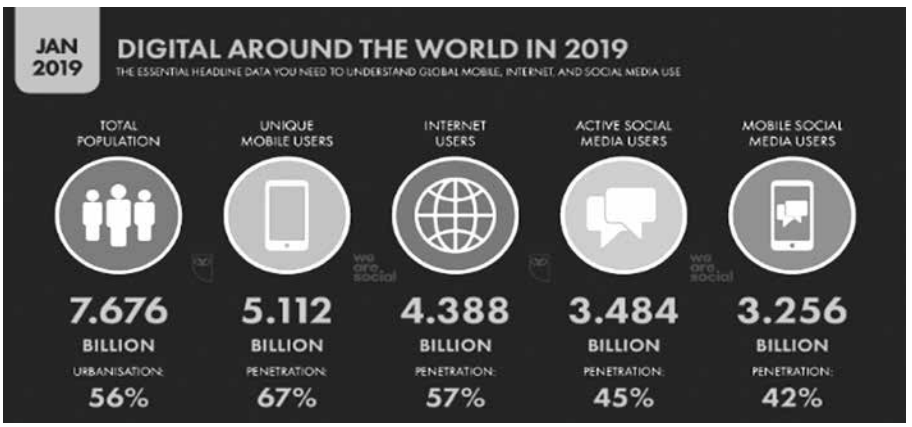
The evolution of advanced information environments is rapidly creating a new category of possible cyber aggression that involves efforts to manipulate or disrupt the information foundations of the effective functioning of economic and social systems. RAND researchers are calling this growing threat virtual societal warfare in an analysis of its characteristics and implications for the future.[6] There analysis suggests

6 Mazarr, Michael J., Ryan Michael Bauer, Abigail Casey, Sarah Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*, Santa Monica, Calif.: RAND Corporation, RR-2714-OSD, 2019. As of January 14, 2020: https://www.rand.org/pubs/research_reports/RR2714.html

an initial set of characteristics that can help define the emerging challenge of virtual societal warfare, including that national security will increasingly rely on a resilient information environment and a strong social topography, and that conflict will increasingly be waged between and among networks. One of the key findings of the paper is that conflict will increasingly be waged between and among networks. State actors are likely to develop such networks to avoid attribution and strengthen their virtual societal warfare capabilities against retaliation. It will be much more difficult to understand, maintain an accurate portrait of, and hit back against a shadowy global network.[7]

In the last few years there has been a revolution of information warfare and well conceptualised and executed campaigns to allegedly interfere with established democratic systems including influencing the US presidential election. “Fake News” and “Truth Decay” are the new normal alongwith information manipulation, fakery, disinformation and propaganda. Perception management is the key to sway public opinion. Hostile social changes, beliefs and manipulation is a low cost option to target adversaries with harmful social, political, and economic outcomes.

War is no longer the preferred option to change the behaviour of a target country or society. World wide the number of internet and social media users is growing exponentially.



(https://wearesocial-net.s3.amazonaws.com/wp-content/uploads/2019/01/Screen-Shot-2019-01-30-at-11.58.23.png)

7 Ibid

There are 5.11 billion mobile users in the world of which 3.48 billion people use social media spending an average of 6 hours 42 minutes online everyday. 47% of Indians use social media.[8] Various nations and watchdogs have raised major concerns with regard privacy and data sovereignty, fake news and many other negative impact of mobile and internet usage, despite the ills people are staying connected and use of social media platforms is a must. The digital world has many advantages but is also a domain which can be easily and effectively exploited to change the behaviour of people, society and nation leading to Sun Tzu's thought of " Winning without fighting".

The role of social media platforms such as Facebook, Whatsapp, Tik Tok in influencing nations with their own narratives is well documented. Many nations are known to have allegedly used misinformation fake news and narratives to propagate their interests and gain political leverage in specific countries. As per a Rand report U.S. intelligence services have concluded that Russia employed such techniques to influence the 2016 election, and Moscow continues to employ them—sometimes brazenly despite U.S. warnings—in the United States and Europe. As significant as these developments have been, they may only represent the beginning of what an aggressive nation can accomplish with techniques and technologies designed to disrupt and shape the information environment of a target country.[9] New age technologies, in particular artificial intelligence, virtual and augmented reality, Big Data and use of Dark web provide easy access and ample opportunities to inimical elements to wage a silent, low cost war on an adversary. Non state actors can exploit these technologies to achieve their ends.

Most people think that they live in an interconnected networked world with information at their fingertips or voice command. Society is only recognising the many advantages of the information domain, they have yet to feel the full impact of the infosphere, especially a war in the infosphere which has the ability both to paralyse nations as also change

the way a society thinks and feels, change the values and behaviour of people, society and nations. The initial hints of what may lie in store

8 https://wearesocial.com/global-digital-report-2019
9 https://www.rand.org/pubs/research_reports/RR2714.html

has already been witnessed among many countries, mainly the large democracies as they are more open and vulnerable. The exploitation of the infosphere will open unprecedented opportunities for hostile rivals—state or nonstate—to covertly or overtly attack a target nations national interests and assets, cause disruption, delay, inefficiency, and active impose costs. It will provide unrestricted opportunities for virtual aggression that will make countries more persistently vulnerable than they have ever been. Such virtual aggression will force a rethinking of the character of national security and means to safeguard their national character and interests. Simply stated the world is staring at virtual wars waged in the infosphere " Winning Without Fighting". This also implies that nation states create capabilities to protect their sovereignty in the virtual world promulgating international rules, laws and regulations to ensure a stable world order.

***Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)** is a former DGMO, Indian Army and is now Director CENJOWS, New Delhi

CENJOWS

CENTRE FOR JOINT WARFARE STUDIES

(Web site: www.cenjows.gov.in - Email: cenjows@cenjows.gov.in)

APPLICATION FOR LIFE/ ANNUAL MEMBERSHIP

To,

The Director
Centre for Joint Warfare Studies (CENJOWS)
Room No. 65, Kashmir House
Rajaji Marg, New Delhi 110011

Dear Sir,

1. Please register me as a Life ☐ /Annual ☐ member of the Centre for Joint Warfare Studies (CENJOWS).
2. I undertake to abide by the Rules and Bye Laws of the Institution.
3. My particulars are given below:-
   (a) Name in full …….....
   (b) Address:-
      (i) Office/Unit…….....
      Pin Code …… Phone No …….....
      (ii) Permanent/Residential …….....
      …….....
      Pin Code…..... Phone No.....
      Mobile No (Optional)…….....
      (iii) Email …….....

   Optional Fields

   (c) Parent Service Army/Navy/Air Force/Civil Services …….....
   (d) Rank/ Designation…..…….. (e) Decorations ……..…. …….…
   (f) Appointment ……..... (g) Personal Number …..……
   (h) Date of Commission ……..…..... (j) Serving/Retired……..…..
4. Areas of expertise or interest:-
   (a) …….. …….....
   (b) …….....
   (c) …….....

5. Any other information that may be of interest to the CENJOWS (including important exposures):-

……

……

6. Proof of my identity (Copy of passport/ voters ID Card/ PAN Card/ Iden Card) will be produced after approval of membership.

7. The following are enclosed:-

(a) Demand Draft/Cheque in favour of CENJOWS payable at New Delhi.

(i) DD/Cheque No……..…… dated…….....

(ii) Amount …….....….....….

(iii) Drawn on ……. Bank.....

(b) Two stamp sized photographs for membership card.

Place : …….....…… Yours faithfully,

Date : …….....……..

FOR OFFICE USE ONLY

Identity Card/Document No: …….. To be verified by Secretary.
New Delhi
Date …..... ……. Secretary, CENJOWS

Accepted/Rejected

Membership Number ……. …….
Place: New Delhi

Date:.....…….....

Director CENJOWS

Note:-

1. Life membership is open for all serving and retired personnel of the Armed Forces, Government Ministries, Academia, members of other think tanks and others interested in studying defence and military strategy.
2. Membership Fees:-

(a)	Life Membership:-		
	(i) Serving/Retired Officers	-	Rs 1,500/-
	(ii) Civilians	-	Rs 10,000/-
(b)	Annual Membership	-	Rs 1,000/-

NOTE

CENJOWS-IMR EVENTS CALENDAR 2019

The Best of Defence Conferences & Exhibitions in India

26-27 Feb 2020, Devlali, Nasik

21-22 May 2020, New Delhi

20-21 Aug 2020, New Delhi

17-18 Sep 2020, New Delhi

October 2020, New Delhi

7-8 Jan 2021, New Delhi

Showcasing & Networking

CENJOWS' Conferences & Exhibitions are developed for professionals and industry to keep them abreast of the latest operational and industry challenges, developments and insights. Every event is designed to furnish delegates with extensive showcasing and networking opportunities.

Official Support

Ernst & Young are Knowledge Partners for CENJOWS - IMR Events, adding value through their market research.

All CENJOWS-IMR events are held in the best facilities such as the Army's Manekshaw Convention Centre, Air Force Auditorium and the DRDO Auditorium.

Hallmark of CENJOWS

The hallmark of CENJOWS-IMR events are senior speakers and delegates – decision makers and serving officers from the Defence Services, Paramilitary, Government, DRDO scientists and top industry executives who are fully conversant with current equipment and technology requirements.

Reports on previous editions of events are also available.

For more information on Sponsoring, Exhibiting, Speaking or Attending please contact

Chetan Sharma | Mob: +91-9582649664 | Email: **chetan@imrmedia.in**

Visit https://cenjows.gov.in