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

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

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

Making Sense of Grey Zone Warfare

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

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

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

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

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

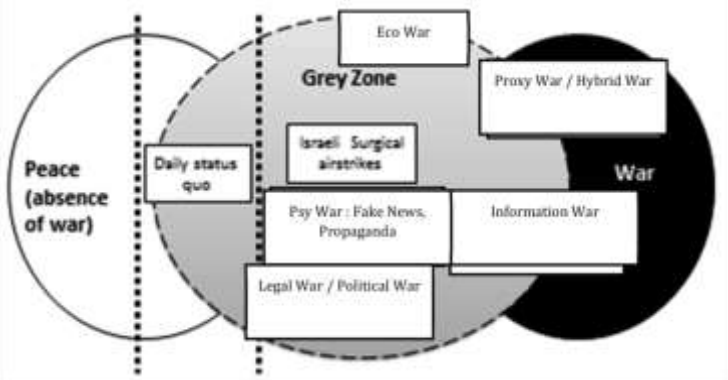


Figure 1: The Grey Zone

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

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

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

Important instances of Grey Activities against India

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

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

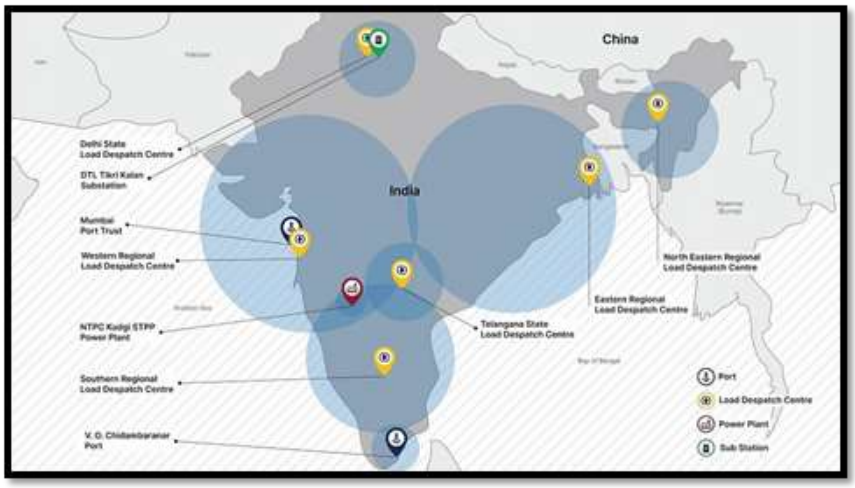
The cyber attack on the country's Power Grid by Chinese hackers once again grabbed headlines when 'Recorded Future's Insikt Group', a Massachusetts based cyber security firm, released a report on the details of the cyber-attacks on India. From mid-2020 onwards, Recorded Future's midpoint collection revealed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

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

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

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

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



Map 1 : Regional Load Despatch Centres

Map 2: Conflict Areas between India and China

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

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

Recommended Approach

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

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

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

Conclusion

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

Conflict Prevention, Conflict Management, and Conflict Termination Strategy.

Endnotes

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

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

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

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

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

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

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

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

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

[9] Ibid.

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

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

[12] Ibid

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

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

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

[16] ibid.

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

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

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

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

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

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

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

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