CENTRE FOR JOINT WARFARE STUDIES

GL/12/24

GREY ZONE WARFARE

BY

LT GEN DUSHYANT SINGH, PVSM, AVSM (RETD)

ORGANISED BY CENJOWS
6TH JUNE 2024

GREY ZONE WARFARE
BY LT GEN DUSHYANT SINGH, PVSM, AVSM (RETD)
ORGANISED BY CENJOWS ON 6TH JUNE 2024

The landscape of warfare is evolving, with an increased concentration of conflicts within the grey zone. This intensity has surged due to emerging niche technologies, making such conflicts increasingly non-attributable. Grey zone warfare is becoming more unpredictable and capricious. An example of this is the incident when "Mumbai went dark" three months after the Galwan clash, which was a coordinated attack on the electrical grid. Historically, all four grids have never been disrupted simultaneously, but in 2020, they were. Speculations link this attack to a China-sponsored hacking agency. In February and June 2020, India's critical infrastructure, including airports and seaports, faced a swarm of over 40,000 hacking attacks by non-state groups allegedly operating from China.

In this context, it is essential to understand the three constants of international relations:

- Conflict and peace efforts
- Environment
- Tools

Several drivers of conflict exist, with national interest and the cost of war being paramount. Technology also plays a crucial role and needs constant updating as it quickly becomes obsolete.

Understanding the definition of wars is vital:

- **Unconventional Warfare (UW):** A broad term for military and quasi-military operations that are not conventional warfare. The goal is to coerce, disrupt, or overthrow a government or occupying power by operating with an underground, auxiliary, or guerrilla force in a denied area.
- **Western Construct of War:** According to Webster, war is the state of open and declared, hostile armed conflict between states or nations. The UNGA Resolution 3314 (1974) defines aggression as the use of force by a state against the territorial integrity or political independence of another state, or in any other manner inconsistent with the UN Charter.
- **Hybrid Warfare:** Combines kinetic and non-kinetic methods to achieve political goals while avoiding direct, large-scale military conflict. It has been prominent since Russian operations against Ukraine in 2014.

When discussing threats to India, it is crucial to highlight the conventional (Conv), unconventional (Unconv), hybrid/grey, and nuclear (nuc) threats from China, Pakistan, and other players. India's national interests focus on unhindered economic growth, the wellbeing of the people, and security against both external and internal threats. The toolkit of grey zone warfare includes:

- Information operations – media and social media
- Cyber-attacks
- People's war, exemplified by the Arab Spring and Gene Sharp's "From Dictatorship to Democracy"
- Private military contractors
- Terrorism
- Lawfare

International examples of grey zone conflicts include:

- Russia – Ukraine
- Israel – Hamas
- Iran – Israel
- Syrian War
- Iran – Saudi Arabia (Houthi Rebels)
- US against Russia
- China – Taiwan

Regarding Russia-Ukraine war, it started with a grey zone context, but then the grey zone element got enmeshed with the conventional conflict.

The Need for India to be Prepared for Grey Zone Threats

India faces potential maritime threats, and national interests such as unhindered economic growth and the wellbeing of its people are crucial. Budget constraints persist, but strategic approaches are essential. Taiwan is currently the world's most affected victim of grey zone warfare. China has established border villages; India could consider similar measures. For instance, the Mansarovar region, historically more connected to India, could be a focal point for counter-grey zone strategies. Reports indicate China has spent at least $6 billion on media campaigns against competitive countries.

Way Ahead for India

1. Involvement of civilians and military personnel in grey zone warfare.
2. Emphasizing the energy sector to enrich the economy, vital for national wellbeing.
3. Utilizing both hard and soft power approaches.
4. Focusing on cost-effectiveness.
5. Combining capabilities across all domains (military, diplomatic, etc.).
6. Developing a robust network.
7. Remaining within the OODA (Observe, Orient, Decide, Act) loop.
8. Establishing separate policies or structures for coordinated team efforts, such as a National Cyber Force.

9. Promoting more apolitical structures like the election commission.

The Analysis

Multi-Domain Operations (MDO) have become the basic norm of conflicts in the modern times. Grey zone warfare elements constitute the options used to negate the influence of MDO. MDO indicates the involvement of state and non-state actors and employs both hard and soft power through conventional and unconventional means. Key domains include water, energy, air, sea, land, and space, alongside economic, legal, political diplomacy, health/bio-terrorism, electromagnetic spectrum (EM), CBRNE (chemical, biological, radiological, nuclear, and explosives), and information/cyber domains. The interdependence of these domains and the increasing relevance of cognitive aspects in grey and hybrid warfare are emphasised in the talk, along with the blurring lines between military and civilian roles.