Date –6 March 2024

GREY ZONE WARFARE

THIS ARTICLE COVERS 'DAILY CURRENT AFFAIRS' AND THE TOPIC DETAILS OF "GREY ZONE WARFARE".THIS TOPIC IS RELEVANT IN THE "INTERNATIONAL RELATIONS AND INTERNAL SECURITY" SECTION OF THE UPSC CSE EXAM.

WHY IN THE NEWS?
On the final day of the 2024 Raisina Dialogue, India's Chief of Defence Staff, General Anil Chauhan, stated that grey zone warfare is the latest type of informal warfare.
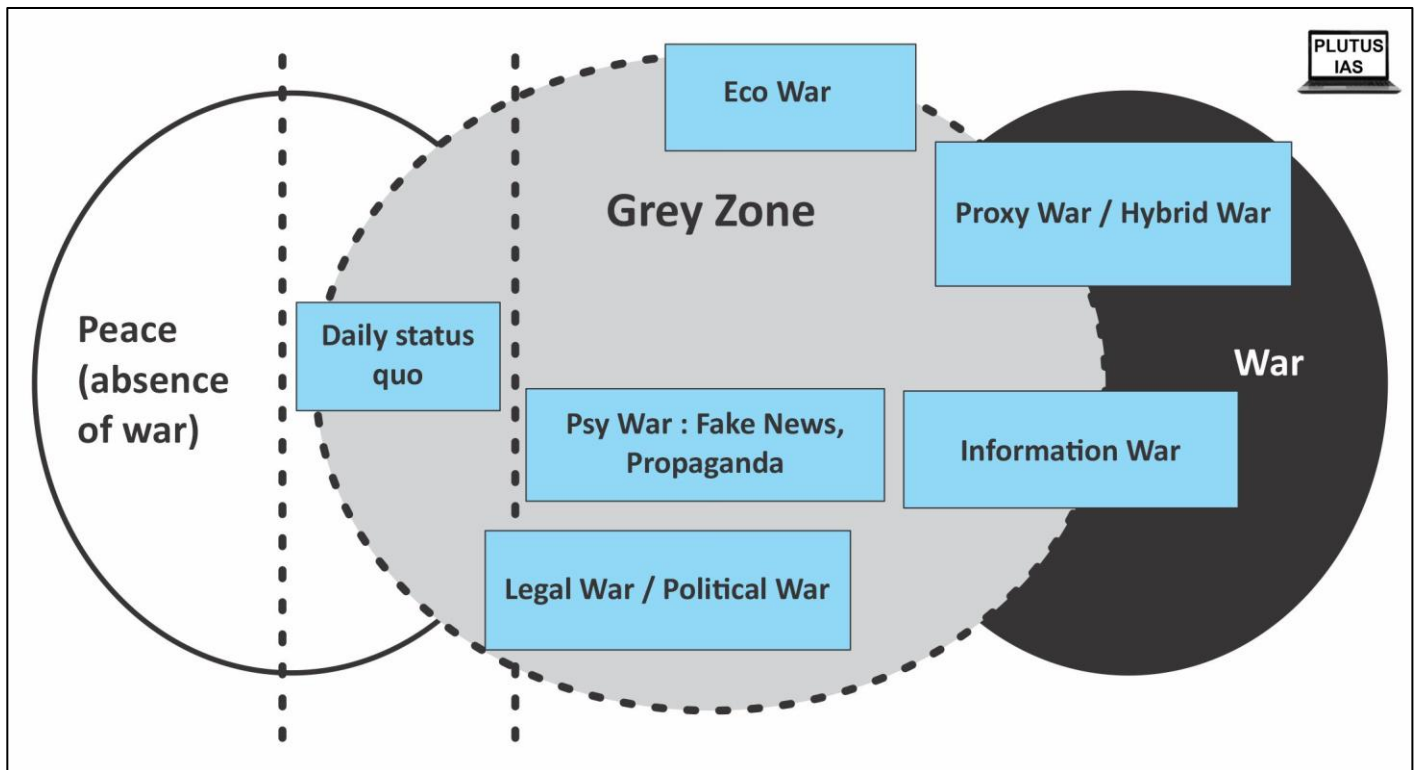
ABOUT GREY ZONE WARFARE

Grey zone warfare refers to a form of conflict that operates in the ambiguous space between peace and war. In this intricate domain, state and non-state actors employ a range of unconventional strategies to achieve strategic objectives without triggering a traditional military response. This article delves into the nuances of grey zone warfare, examining its characteristics, tactics, and implications for international security.

UNDERSTANDING GREY ZONE WARFARE:

- **Blurring the Lines**: Grey zone warfare is characterised by its ability to exploit the ambiguity between peace and war. Unlike conventional conflicts with clear delineations, grey zone tactics involve actions that fall short of open hostilities but are aggressive enough to influence the targeted entities significantly.
- **Unconventional Tactics**: The toolkit of grey zone warfare is diverse, encompassing cyberattacks, disinformation campaigns, economic coercion, proxy warfare, and more. These methods allow aggressors to achieve their objectives while maintaining plausible deniability, making it challenging to attribute actions to specific actors.

THE AMBIGUOUS NATURE OF GREY ZONE CONFLICT

- **Subtle Aggression**: Grey zone warfare is marked by its subtle and covert nature. Adversaries engage in activities that create ambiguity, making it difficult for the international community to discern whether a particular action is an act of war or falls within the realm of peaceful activities.

- **Ambiguity in Attribution**: One of the key challenges in responding to grey zone tactics is the ambiguity in attribution. Determining the responsible party behind cyberattacks, information operations, or proxy activities becomes a complex task, often hindering effective countermeasures.

TACTICS EMPLOYED IN GREY ZONE WARFARE

Cyber Operations:
Grey zone actors leverage cyber capabilities to infiltrate, disrupt, or manipulate targeted systems. Cyberattacks on critical infrastructure, espionage, and ransomware campaigns are common tactics employed in this domain.

Unconventional Warfare – Employing non-traditional military strategies like guerrilla warfare, sabotage, or asymmetric assaults through the utilisation of smaller, specialised units or unconventional military forces is a component of Irregular Warfare.

Strategic Legal and Diplomatic Tactics – China exercises caution in capitalising on legal or diplomatic ambiguities, utilising international institutions, or manipulating alliances to diminish the targeted country's standing on the global stage. Simultaneously, China provides justifications for its actions based on established principles and conventions of law.

Disinformation Campaigns:
Manipulating information and spreading false narratives play a crucial role in grey zone warfare. Disinformation campaigns aim to sow discord, influence public opinion, and destabilise political systems without resorting to overt military actions.

Economic Coercion:
Economic tools, such as sanctions, trade restrictions, and financial manipulations, are frequently used to coerce and pressure adversaries. These actions can have far-reaching consequences on a nation's stability and well-being.

Proxy Warfare:

Grey zone conflict often involves indirect or proxy actions, wherein states support non-state actors to achieve their objectives. This allows aggressors to maintain plausible deniability while exerting influence in a region.

IMPLICATIONS OF GREY ZONE WARFARE

Challenges to International Security: Grey zone tactics challenge traditional notions of security, as they exploit vulnerabilities in political, economic, and social systems. This form of warfare requires a holistic understanding and response that goes beyond conventional military frameworks.

Erosion of Norms and Rules: Grey zone warfare blurs the lines of established norms and rules governing international conduct. This erosion of norms poses challenges to the existing international order and institutions, raising questions about the effectiveness of current frameworks.

Persistent State of Conflict: The subtle and prolonged nature of grey zone warfare contributes to a persistent state of conflict. Without clear triggers for traditional military responses, affected nations find themselves engaged in an enduring struggle without a formal declaration of war.

CHINA'S GREY ZONE STRATEGIES VIS-À-VIS INDIA

Maritime Actions in the South China Sea – China utilises both naval and civilian vessels to assert dominance in the South China Sea, creating tensions with neighbouring nations, including India.

Development of Infrastructure in Border Regions – China engages in the construction of infrastructure and the establishment of villages near India's borders, reinforcing territorial claims and securing strategic advantages.

Financial Commitments to Digital Technologies – China channels investments into applications, media, and diverse digital platforms within India. This involvement in the digital realm has the capacity to shape public opinions and narratives.

CASE STUDY: GREY ZONE WARFARE IN THE INDO-PACIFIC:

Territorial Disputes: The Indo-Pacific region has become a hotspot for grey zone activities, with territorial disputes among nations leading to unconventional tactics such as maritime coercion, cyber intrusions, and disinformation campaigns.

South China Sea Scenario: China's actions in the South China Sea exemplify grey zone tactics. The construction of artificial islands, military presence in disputed waters, and assertive maritime activities demonstrate the use of subtle aggression to advance strategic interests without triggering a conventional conflict.

PRELIMS PRACTISE QUESTIONS

Q1. Consider the following statements regarding Grey Zone Warfare:
1. Ransomware campaigns are one of the common tactics used in grey zone conflict.
2. The erosion of norms and rules is the key implication of it.

Which of the statements given above is/are correct?
(a) 1 only

(b) 2 only
(c) Both 1 and 2
(d) Neither 1 nor 2

ANSWER: C

Q2. What is the key objective of disinformation campaigns in grey zone warfare?
(a) Promoting peace and understanding
(b) Destabilising political systems
(c) Encouraging military conflict
(d) Enhancing international cooperation

Answer: B

MAINS PRACTISE QUESTIONS

Q1. In a world where social media manipulation and disinformation campaigns are prevalent, how can India safeguard its national security and social fabric against these tactics employed in grey zone warfare?

Q2. How can traditional diplomatic tools and international legal frameworks be adapted and leveraged to address the challenges posed by grey zone warfare in the Indian context?

Himanshu Mishra