Mains Practice Question

Q. Hybrid Warfare is a multi-pronged warfare methodology, thus to negate it, the response should also be holistic in nature. Discuss. (250 words)

06 Jan, 2021 GS Paper 3 Internal Security

Approach

- Introduce by briefly explaining hybrid warfare.
- Highlight the implications of hybrid warfare.
- Discuss the measures to combat hybrid warfare.
- Conclude suitably.

Introduction

Hybrid warfare refers to the use of unconventional methods as part of a multi-domain warfighting approach. In Hybrid warfare, apart from conventional military tactics, non-military tools are used to achieve dominance or damage, subvert or influence.

These tools may include information pollution, perception management and propaganda. These methods aim to disrupt and disable an opponent's actions without engaging in open hostilities.

Body

Characteristics of Hybrid Warfare

- **Multi Domained:** This warfare is a combination of activities, including disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure and military actions.
- **Maximum Damage With Minimum Effort:** It tends to target areas which are highly vulnerable and where maximum damage can be caused with minimum effort.
- **Deploying Non-State Actors:** It usually involves non-state actors indulging in subversive roles supported by states in order to exonerate themselves of any involvement if their activities are detected.

Recent Usage

- **Israel-Lebanon War (2006):** In this war Hybrid warfare was used by the Hezbollah group. It employed a host of different tactics like guerilla warfare, innovative use of technology and effective information campaigning.
- **By Russia (2014):** Hybrid warfare techniques were deployed against Ukraine in the annexation of Crimea. It involved a combination of activities, including disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure etc.
- **By China:** Unrestricted Warfare, a publication by China's People's Liberation Army, talked about hybrid warfare and the need for a shift in the arena of violence from military to political, economic and technological.
    - Recently it was reported that the Chinese company Zhenhua Data Information Technology

Co. Limited is monitoring over 10,000 Indian individuals and organisations in its global database of foreign targets.

Threats Emanating From Hybrid Warfare:

- **Cyber Attacks:** This may include attacks on critical infrastructure like power grids, water supplies, business systems, and defence systems. These may be used to disrupt economic activities, undermine institutions, and discredit political leadership and the intelligentsia.
- **Evolving Nature of Terrorism:** The idea of Hybrid Warfare encourages new forms of terrorist attacks such as ‘lone-wolf’ attacks and creation of ‘sleeper cells’. These attacks are extremely difficult to detect.
    - Adversary could also act on the lines of radicalization of the population, which leads to issues like Communalism, Naxalism and Separatism in the long run.
- **Undermining Democracy:** The foreign government may manipulate the data, spread propaganda and misinformation and influence democratic systems like elections through use of social media, websites, advertisements etc.
    - Use of techniques from campaigning through the media and social networks to securing financial resources for a political group may indirectly influence the outcome of an election in a direction that favors the adversary's political interests.
- **Disinformation and Fake News:** An adversary can create a parallel reality and use falsehoods to fuel social fragmentation. It could disorient the public and make it difficult for a government to seek public approval for a given policy or operation.

Holistic Responses to Combat Hybrid Warfare

- **Adopting multinational frameworks:** Threats from hybrid warfare are an international issue, so should be the response. National governments should coordinate a coherent approach amongst themselves to understand, detect and respond to hybrid warfare to their collective interests. Multinational frameworks should be developed to facilitate cooperation and collaboration across borders.
- **Institutional measures:** To keep vulnerabilities in check and estimate possible hybrid threats, conducting self-assessments of critical functions and vulnerabilities across all sectors and ensuring regular maintenance. For example, regularly upgrading critical Fintech systems in the country.
- **Training of armed forces:** In hybrid warfare, armed forces have a dual role in protecting civilian population and disabling enemy. Thus it needs to upgrade itself by adopting the following:
    - Training in special battle techniques, as well as conditioning to overcome urban combat stress.
    - Training in use of technological tools such as smart robots, Unmanned Aerial Vehicles (UAVs)
    - Deploying Intelligence tools like Real Time Situational Awareness (RTSA) for precise operations.
- **Strengthening the democratic institutions:** This helps the government negate various forms of hybrid warfare such as disinformation and radicalization. Inclusion of Civil Society Institutions such as think tanks multiply the government’s capabilities to counter such threats.
- **Investing in Journalism to raise media literacy:** It has been often reported that uses of the term “hybrid threats” by the media are often inaccurate. As a result, investing in journalism will indirectly help citizens in understanding the threat in a better way.

Conclusion

Thus, the governments across the world should establish a process to develop a national approach of self-assessment and threat analysis. Institutionalizing a process regarding threat and vulnerability information will enhance hybrid warfare early warning efforts, assist resiliency efforts, and may even have a deterrent effect.

PDF Refernece URL: https://www.drishtiias.com/mains-practice-question/question-788/pnt