Learnings from the world's first Hybrid War - Is India ready ?

New Threats, Increased Complexity, and The Way Ahead for India

August - 2022

Freedom of Expression, Trust and Safety on Internet

www.indiafuturefoundation.com

INDIA FUTURE
FOUNDATION

TABLE OF CONTENTS

The ongoing war between Russia and Ukraine is undoubtedly the first hybrid war the world has seen. Among other things, this war has taught important open lessons that nations can take cognizance of and, more so, India, considering the peculiar position that India is placed in. This paper invites discussions on the same "Lessons India can learn from the first hybrid war."

Before getting into the specifics of this paper, it would be necessary to understand why the ongoing war is called the first hybrid war and what a hybrid war means.

Hybrid Warfare

Hybrid warfare refers to the combined employment of conventional and unconventional means of force and subversion/coercion to win a war. These instruments or tools are employed in unison, typically discreetly, to exploit an opponent's weaknesses and create synergistic results.

No matter how different the capacities of the contending parties or opponents are, recent studies[1] on the conflicts in Afghanistan and Iraq show us how expensive all-out warfare can be in terms of human, economic, social, and political costs.

All-out conflicts may be ineffectual even against nations with comparatively fewer resources and influence due to the rapid growth of technology and the rise of asymmetric warfare. Thus, winning can turn out to be very challenging, even for the strongest of nations.

This means that it is technically possible that in the future, the nature of how wars a fought will be completely different from how a war was fought in the past. This still has a solid connection to the theory of war.

According to the legendary military thinker Sun Tzu, the greatest art of war is to subdue the opponent without engaging in combat.

[1] https://watson.brown.edu/costsofwar/

Difference between a Hybrid & a Conventional War

Wars are fought even today between nations by soldiers, but where it has changed is the use of technology to carry out a range of activities like espionage and managing public opinion, and that is what a hybrid war is. While soldiers will fight wars with weapons, the technology employed to steer the war in one's favor makes a war hybrid. With advancements in technology, its use in war will undoubtedly increase, and wars in the recent past have attested to this fact.

Combining kinetic weapons with non-kinetic strategies aims to harm a belligerent state as effectively as possible. Hybrid warfare has two separate traits in addition. The distinction between war and peace is first made unclear. This implies that it is challenging to pinpoint or distinguish the war threshold, as it becomes more challenging to operationalize war. It becomes elusive.

Despite being simpler, less expensive, and less dangerous than kinetic operations, the threshold is lower in hybrid warfare and acts as a catalyst so that direct overt violence pays off. Instead of sending tanks into another country's territory or scrambling fighter planes into their sky, sponsoring and promoting disinformation in cooperation with non-state actors is much more practical. While the costs and hazards are far lower, the harm remains, and the results are more rewarding.

Ambiguity and attribution are connected to hybrid warfare's second distinguishing feature. Hybrid attacks typically include much ambiguity. The hybrid actors purposefully generate and increase this obscurity to make it more difficult to attribute the actions to them and for the opposite party to respond. In other words, the targeted nation is either unable to identify a hybrid attack or is unable to link it to a possible sponsor or perpetrator state. By taking advantage of lower detection and

attribution thresholds, the hybrid war's aggressor hinders the targeted state's ability to formulate strategies and policy responses.

Conflict dynamics become unclear due to hybrid warfare since it allows an adversary's security to be compromised simultaneously on two fronts. This pertains to the main goals of hybrid warfare as well. On the capacity front, the targeted state's weaknesses are exploited to the extent that they are visibly and functionally weakened in the PMESII (political, military, economic, social, information, and infrastructure) spheres.

The 1st Hybrid War?

“This is happening for the first time in history”

- Victor Zhora

In a press briefing on the cyber-conflict between Russia and Ukraine, Victor Zhora, the deputy head of Ukraine's cyber security agency SSSCIP, stated that the state is engaged in a war both online and on the ground. The ministry (SSSCIP) claims that its infrastructure and government networks are always the targets of cyber attacks, with specific individuals also being singled out. It asserted that while its cyber defenses repel most attacks, the confrontation with Russia was unprecedented and referred to as a "hybrid war."

A key question here is: Is India ready for any such actions?

"The Russia-Ukraine conflict is the first true instance of hybrid warfare and has a lot of lessons. We need to focus more on research and development."

- Air Chief Marshal, Vivek Ram Chaudhari

Is India Ready – Protecting our Critical Information Infrastructure

While the ongoing war between Russia and Ukraine has shown the extent to which technology can be used in modern warfare, this war has also shown that if technology is used in the right manner, even advances of a stronger nation can be thwarted. So what's there for India as a nation to learn from the first hybrid war?

Before dwelling on the details, it is essential to understand the strategic position of India. Recently, the country has been at the receiving end of cyber attacks from its neighbors. Skirmishes with its neighbors, in an attempt to protect its borders, is also not new. Against that background, even if chances of a full-scale war are not imminent, increasing instances of cyber-attacks on India cannot be ruled out.

Many nations have invested in digital infrastructure; for instance, India has Aadhaar (for identity) and the Unified Payment Interface (for payments) for better governance. However, more work must be done to create and protect the physical infrastructure that enables connectivity and last-mile connectivity so that the government and its citizens continue to benefit from such innovations, even in the case of an exigency.

At the same time, discussions about trustworthy data-sharing mechanisms are also needed. Protocols for the security of servers and general crisis management in the event of a cyberattack also need to be considered more. Given its border issues, India needs to take a cue from the ongoing war and consider constructing and integrating digital resilience into all facets of its operations.

Tech sanctions and economic coercion

Russia significantly depends on the American semiconductor industry for its thriving domestic technology, industrial production, and aerospace sectors. However, the imposition of sanctions' tends to hurt Russia's "capacity to compete economically" and may have even dealt Putin a severe blow towards his long-term strategic goals.

To determine the direction of its security strategy and discourage its enemies, India must consider the function of tech sanctions and their influence on tech supply chains in light of this experience and the crisis in Ukraine.

Security alliances

India will need to take care of itself in such a situation. There will also always be restrictions on India's international security alliance relationships and defense cooperation because it is not a member of any formal security alliance, and it is unlikely it will ever be. As a result, New Delhi will eventually need to define a path based on independence to safeguard and develop its security objectives.

Lessons to learn from the Ukraine war

India needs to rethink how the next war is to be fought. We must review our command-and-control structures and where they fit in if a hybrid war becomes a reality.

Today we neither have an integrated command structure consisting of purely non-contact war elements nor hybrid Corps and divisions that could employ all elements of a hybrid war together. Thus India needs to create an integrated command that can have all elements of hybrid war under a single commander. The bricks from this command can be plug-and-play for air, ground, and maritime campaigns.

Key Takeaways for India

- India should learn from the recent Ukraine crisis that no other nation will send troops to support New Delhi if its neighbors start a war.
- The way forward is to emphasize improving our financial capabilities and producing equipment here at home. We cannot rely on different nations to meet our defense requirements, including those for tools and fighting a war.
- The Russia-Ukraine situation has amply demonstrated the value of not relying on another nation for military hardware. The government should vigorously advocate for its R&D in the armed forces and prefer such goods and businesses to create systems based on in-house research and technology.
- This also means that India should become self-reliant, but in a connected world, it should build strong relations with friendly nations
- India also needs to strengthen its relationship with QUAD countries so it can bank on them in case of an eventuality like a hybrid war.
- India should be a solid proponent and look at technology and skill-sharing agreements with countries that are considered more proficient, in this field, like the USA and the UK.
- India needs to deepen its cooperation with the US in fields like trade and investment, defense and security, education, science and technology, cyber security, high-technology, civil nuclear energy, space technology and applications, clean energy, environment, agriculture, health, and so on.
- India also needs to strengthen its collaboration in artificial intelligence (AI), machine learning (ML), and similar new technologies and data regulation as these topics become more important for national security.
- India will hold the G20 Presidency from 1 December 2022 to 30 November 2023 and host the 18th G20 Summit in 2023. India should propose a joint training initiative for Computer Emergency Response Teams (CERTs) of the Indo-Pacific countries. The initiative would bring together CERT officials in the region to undertake collaborative learning and skill development and to share best practices to enhance timely and secure information sharing under the Information Exchange Policy developed by the Forum for Security Incident Response Team. India should also propose a new digital governance framework that is inclusive and trust-based.
- Given India's unique position, India should take the leadership position among G20 nations so that it can be in a position to develop alliances across various fields for cooperation.

Threat from China?

China has implemented a "Strategic Support Force" that has integrated cyber, electronic, information and space. It is neither a copy of the western nor Russian model of integrating all components of non-contact warfare. It is innovative and path-breaking.

Partnerships to Surmount Hybrid Threats

Experts have put forth various policy and strategic approaches in light of hybrid warfare's complex dynamics and nature. Some of these involve taking careful precautions to identify, deter, combat, and respond to hybrid threats. However, given that hybrid warfare is based on the information, cognitive and social domains, any set of remedies devoid of the development of confidence and trust are likely to fall short of serving as potent countermeasures.

India Future Foundation

Freedom of Expression, Trust and Safety on Internet

🌐 www.indiafuturefoundation.com

☎ +91-1244045954, +91-9312580816

📍 Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram, Haryana, India – 122003