Hybrid threats in the national security context of Nepal

Padam Kumar Angbo

Abstract

Of late, hybrid warfare has emerged as a widely contested but practically tested war strategy anticipated in the future. This paper revolves around strategies to deter, mitigate and counter hybrid threats to national security in the context of Nepal. Prevailing geopolitical and geostrategic environments exhibit that different actors, including state and non-state hybrid strategies pose a clear challenge to Nepal's national security interests. Hence, there is a need for a national security strategy to counter hybrid threats which demands fresh thinking, expanding the traditional enemy-centric threat assessment and response. But the general understanding of hybrid warfare is underdeveloped because hybrid means are ambiguous and complex, such as unorthodox, unpredictable and constantly changing. Ultimately, developing and implementing effective national security policy, ensuring political stability, zero tolerance policy on corruption, good governance, economic and resources development, trusted law enforcement, effective stakeholders including security and intelligence system, building resilience are the best ways to prevent a hybrid war before it erupts. This article argues that Nepali Army, as a key responder, too needs to have an updated military doctrine and strategy on its role in countering it

Keywords: hybrid threats, conflicts, warfare, national security, war strategy, military doctrine

Hybrid threats

Of late, Hybrid Warfare (HW) has emerged as a widely contested but practically tested war theory. For example, Russia's use of hybrid tools in three instances indicates that it has successfully applied concepts of hybrid war, as expounded by Gerasimov, in furthering its strategic and political aims (Kohli, 2018, pp. 187-188). Consequently, many of the nations' security strategy documents have already incorporated it. In the UK's 2015 Strategic Defense and Security Review, hybrid threats were classified as a 'Tier One' risk to national security and hybrid attacks on allies as a 'Tier Two'(UK's, National Security Strategy & Strategic Defense & Security Review 2015, p. 85). Both state and non state actors have successfully implemented the hybrid strategy to counter relatively mightier state militaries.

Therefore, its relevancy is likely to grow as nation–states, including Nepal are likely to face more hybrid threats in future primarily due to clash of interests. Actors will have more access to means that can target more vulnerabilities, more cost- effectively. As scholars Brown, Lackey, and Forester (2019, p. 35) aptly write, "we are at strategic inflection point. A hypercompetitive global environment coupled with accelerating technological, economic and social change has resulted in an incredibly challenging and complex twenty-first century operating environment." In such a politico military strategic environment, the evolving theory of HW merits a critical detailed assessment.

Apparently, it should form an integral part of Nepal's security strategy. Foregoing in view, this paper aims to help generate a conceptual clarity required for officers to help understand and think about how to deter, mitigate and counter hybrid threats to national security in the context of Nepal.

Considering the indispensability of national security in changing global context, this paper outlines a strong nation –state's hybrid threats in respective four parts of this paper.

a. Notion of theory of HW

b. Characteristics and challenges

c. Hybrid Threat Scenario in the context of Nepal

d. The way ahead

Notion of hybrid war

As a Swedish analyst Gunneriussan (2017, p. 111) generously suggests, the term hybrid warfare has "travelled a lot in definition". In fact, there is no universally accepted definition of the term HW. Experts use these terms, including hybrid threats, warfare activity, operations tactics and conflict interchangeably. There are diverse perspectives on hybrid war.

Hoffman (2007, p. 8) proffers that "hybrid warfare incorporates a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder".

Similarly, Korybko (2007) noted hybrid warfare as an attack against Russia, the Eurasian concept and the initiatives to implement One Belt One Road and China.

However, Gerasimov states, "What constitutes a weapon in this grey area no longer has to go 'bang'. Energy, cash - as bribes - corrupt business practices, cyber attacks, assassination, fake news, propaganda and indeed military intimidation are all examples of the weapons used to gain advantage in this era of 'constant competition" (MCDC, 2019, p. 1)

In addition, Liang and Xiangsui state that **"**everything is changing. We believe that the age of a revolution in operating methods, wherein all of the changes involved in the explosion of technology, the replacement of weapons, the development of security concepts, the adjustment of strategic targets, the obscurity of the boundaries of the battlefield, and the expansion of the scope and scale of non-military means and non-military personnel involved in warfare are focused on one point, has already arrived" (MCDC, 2019, p. 8).

Israel defines hybrid warfare as a method of social warfare (Sandor, 2019).

Russian strategists use the term 'hybrid war' to refer to alleged US efforts to weaken and ultimately overthrow unfriendly governments, particularly, but not exclusively, the Russian government, using a variety of kinetic and non-kinetic means (Charap, 2016, p. 51). The hybrid threat can be taken for a blend of different forces, such as regular and irregular directed to accomplish productive effects through the military institution for the state.

Cilevics (2018) considers "hybrid threat" a "catch all" notion, used to designate the occurrence of simultaneous security threats. According to the EPRS it may cover various situations, including terrorist acts of Boko Haram, Al-Queda or Daesh, actions against

cyber security, actions of armed criminal groups, such as those of Mexican drug cartels, maritime disputes in the South China Sea, constraints on the use of orbital space, hostile economic acts, such as the blocking of Japanese exports by China in 2010 or covert military operations like the use of "green men" in Crimea. Kumar (2018, p. 2) writes that

> Hybrid warfare has demonstrated that non-state actors with state patronage, like the Iran-backed Hezbollah, Pakistan backed Taliban, US-backed Syrian Democratic Forces, and Russian-backed militias in Ukraine are waging war against states by fighting within the nation and eroding the authority of the state over its territory and resources. Instead of relying solely on irregular tactics, as insurgent groups have done in the past, they have surprised their adversaries with conventional capabilities and the employments of cyber warfare to degrade, disrupt, dislocate, and destroy the ability of a state to fight a war.

Characteristics of hybrid threats

All nations and organizations should be prepared to tackle hybrid threats to their security in changing global context. With progress in science and technology, nation – states and leaderships should be ready with preemptive measures to security on different fronts. Some of the salient features of hybrid war are enumerated below.

a. It operates in the "gray zone" between war and peace, conventional and irregular conflict.

b. It generally, makes an extensive use of proxies.

c. HW may fall short of an outright military attack.

d. It is hard to detect, identify a proper response against hybrid threats.

e. It targets vulnerabilities across societies in ways that we do not conventionally imagine about.

f. It synchronizes its means in new and ambiguous ways.

g. HW exploits creativity, and our understanding of war to make attacks less obvious.

h. A HW campaign may not be seen until it shows effects.

i. It is population/ urban centric.

j. It economizes the use of force by use of cyber tools (Chivvis , 2017, p. 4)

k. Non-state actors demonstrate unexpected levels of military sophistication.

l. Hybrid adversary resorts the law as a weapon (Lawfare)

Challenges to national security

Hybrid threats pose complex and multifarious challenges to national security because, in hybrid conflict, the challenges faced by a nation's armed forces surpass a military challenge. The basic challenge in responding to such a threat is whether to respond to them as acts of war, or as confrontational behavior or whether to respond to them at all. The Taliban's strategy, modus operandi and tactics during the Afghanistan conflict and the Islamic State militia's early campaigns against the governing regimes in Iraq and Syria demonstrate the complexity of hybrid conflict.

Hybrid threat in Nepal's context

Hybrid warfare is designed to exploit national vulnerabilities across the political, military, economic, social, and informational and infrastructure (PMESII) spectrum (Cullen & Kjennerud, 2017, p. 24). In the context of Nepal, we can hypothesize three categories of hybrid threat scenarios. The first scenario is adversary's nonviolent subversion. The second scenario is the non-violent action. The third scenario could be the violent action, including conventional attacks in combination with other kinetic and non kinetic tools to accomplish political objectives. In order to comprehend the above-mentioned scenario, it will be prudent to identify contextual factors which help envisage the vulnerabilities, threats and response. The following contextual factors illustrate our vulnerabilities.

a. Economic / Aid dependency
b. Political instability
c. Erosion of nationalism
d. Cyber
e. Corruption
f. High levels of dependency on strategic commodity items like oil and gas
g. Geo-strategic location
h. Territorial dispute
i. Internal Security issues
j. Critical infrastructure

Hybrid threat instruments

Chinese Colonels Liang and Xiansui (1980) propose that the adversary can employ the following instruments in order to conduct hybrid activities.

a. Cultural
b. Diplomatic
c. Network Intelligence
d. Psychological
e. Technological
f. Smuggling
g. Drug warfare
h. Financial Trade
i. Resources
j. Economic/economic aid incentives
k. Sanctions
l. Media/propaganda
m. Ideology/religion
n. Forced population shifts/migration

Meanwhile, RAND (2018) proffers covert means, unconventional warfare and proxy warfare as hybrid threat instruments. Dubik and Vincent (2018) consider domestic networks and military coercion (short of war) as the potential non-violent hybrid threat instruments. Additionally, the main instrument of hybrid war is the notorious 'fifth column' of agents of influence controlled by adversary.

Conclusion

Prevailing geopolitical and geostrategic environments exhibit that different state and non state actors pose a clear challenge to Nepal's national security from hybrid threats. There is a need for fresh thinking while expanding the traditional enemy-centric threat assessment and response. Unfortunately, as Cullen & Kjennerud (2017, p. 8) argues that "our common understanding of hybrid warfare is underdeveloped and therefore

hampers our ability to deter, mitigate and counter this threat." In any case, hybrid aggression has to be prevented or deterred. Perhaps, it will be too late to defeat a hybrid adversary once prevalence of political, military, social, economic, diplomatic and informational conditions is in enemy's side. Therefore, hybrid threats have to be dealt before they take us by surprise.

But in view of nation's ground realities, how then is it possible to secure a nation from hybrid threats? Hybrid ways and means are ambiguous and complex (unorthodox, unpredictable and constantly changing). Like, the US Army TRADOC states, "The Army cannot predict who it will fight, where it will fight". Moreover, hybrid threats cannot be countered solely by military means. Ultimately, developing and implementing effective national security policy, ensuring political stability, zero tolerance policy on corruption, good governance, economic and resources development, trusted law enforcement, effective stakeholders including security and intelligence system, building resilience are the best ways to prevent a hybrid war before it erupts. Therefore, taking initiative to prevent, counter and respond to hybrid attacks by state or non-state actors, should be accorded priority in Nepal's national security strategy. Nepali Army, as a key responder, too needs to have an updated doctrine and strategy on its role in countering HW.

Recommendations

The potential for hybrid threats to create a paralysis effect in Nepal requires a strategic response. Why strategic approach offers solution to the problem is because countering strategies against hybrid warfare are more often successful than not when they address the 'ends' rather than tackling the 'ways' and 'means'(Kumar, 2017). Foregoing in view, following recommendations are proffered.

a. Strategy. Preparing necessary response to adversary's hybrid threats or attacks require a resolute national effort. All the stake holders including security agencies should be effectively prepared to counter hybrid attacks in any form. To do that, as a first step, "Hybrid threats" be considered in our National Security Strategy. Such strategy essentially will have three broad implications i.e. to detect hybrid threats, deter hybrid aggressors and respond to hybrid attack.

b. Consensus about the threat. Developing and implementing above mentioned national security strategy would require consensus about hybrid threats, HW and its meaning to Nepal's national security. The criticality of cooperation with non-military actors and a thorough understanding of civil-military coordination to achieve unity of effort cannot be overemphasized.

c. Vulnerabilities assessment. As a minimum national government should conduct a self-assessment of critical functions and vulnerabilities across all sectors, and maintain it regularly (Cullen & Kjennerud, 2017, p. 24). National efforts should augment threat assessment activity including non-conventional political, economic, civil, informational tools and capabilities.

d. Prevention. Ensuring political stability, zero tolerance policy on corruption, good governance, economic development and trusted law enforcement, effective stake holders including security

and intelligence agencies are the best ways to stop a hybrid war before it erupts as a security challenge.

e. Natural resources. There is a need for developing the country's natural resources for economic growth, as modern warfare is more than weapons and technology.

f. Capability. Nepal must develop the ability to deter and defeat a variety of complex state / non-state, regular/ irregular potential hybrid adversaries. Capability development includes not only doctrine, training and equipment but also embraces aspects such as civil-military cooperation, cyber defense and human intelligence for countering hybrid threats.

g. Anti-corruption. Tolerance of corruption facilitates adversary's hybrid strategies. According to the 2019 Corruption Perceptions Index reported by Transparency International, Nepal is the 113 least corrupt nations out of 180 countries. As then King Prithvi Narayan Shah said, "Ghush khanya lai thokanya hun "(Corrupt must not be spared, Dibyopadesh, 2059, p. 46). Building integrity is also necessary to enhance anti-corruption efforts.

h. Doctrine. Basing upon National Security Strategy, Nepali Army can develop a comprehensive HW Military Doctrine. When developing doctrine to countering hybrid threats, she can refer various factors including the lessons learned from the past operations /conflicts.

i. Cyber. In Cyber domain, Nepal needs to strengthen own defenses against cyber attacks. Nepal faced around 800 cyber attacks last year 2018. Facets of those cyber attacks included attacks on social media, piracy, identity threat, unauthorized access, website hacking (CAN Federation, 2018).

References

Brown, R. B., Lackey, B.R., & Forester, B.G. (2019). Competing with China for a free and Open Indo pacific, China's new style warfare, *Military Review,* p.35. September- October 2019

Charap, S. (2015). The ghost of hybrid war, *Survival*, 57:6, 51-58, DOI:10.1080/00396338.2015.1116147

Chivvis, C. S. (2017). *Understanding Russian " Hybrid Warfare" and What Can be Done About It* , p. 4 Published by the RAND Corporation, Santa Monica, Calif. Cilevics, B., (2018), *Latvia: Legal challenges related to hybrid war and human rights obligations*, *Report* | Doc. 14523 | 06 April 2018, Retrieved from\ https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en

CAN Federation. (2018). CISCO Global cyber security summit report

Cullen, P. J, & Kjennerrud, E. R. (2017). MCDC countering hybrid warfare project: *Understanding Hybrid Warfare,* p. 8, 24

Dubik & Vincent. (2018). *America's global competitions: The gray zone in context*

Definition of hybrid, Merriam Webster Dictionary, Retrieved from https://www.merriam-webster.com/dictionary/hybrid

Gunneriussan, H. (2017). *Bordieuluan field theory as a instrument for military operational analysis*, Springer international publishing 2017, p 111

Han, Y. (2011). *"Changing security threats" Imagining Asia in 2030, Trends, Scenarios and Alternatives,* p. 349 New Delhi, published by Academic Foundation in association with the Institute for Defense Studies and Analysis (IDSA)

Hoffman, F. (2007). *Conflict in the twenty-first century: The rise of hybrid wars* p. 8 published by the Potomac Institute for Policy Studies, Arlington VA 22203 Retrieved from https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108 pdf

Kohli, N., Hybrid Warfare: The changing character of conflict, Institute for Defense Studies and Analysis, published by Pentagon Press, New Delhi 110049 / 2018; pp. 187-188

Kumar, N. (2018). War beyond rules: Hybrid war and India's preparedness, *CLAWS Journal*, pp. 758-74

Liang Q. & Xiangsui, W. (1980). *Unrestricted warfare, 1980*

Liang & Xiangsui (1999). *Trans-military and non-military forms of warfare* in unrestricted warfare, Beijing: PLA Literature and Arts Publishing House, February 1999

MCDC. (2019*). Countering hybrid warfare project*: *'A deadlier peril', The role of corruption in hybrid warfare*, Information Note, March 2019

MCDC. (2017). *Countering Hybrid Warfare Project: Understanding Hybrid Warfare* MCDC January 2017

Ministry of Information and Communication, Kathmandu, (2059 BS), *Dibyopadesh,* p. 46

NATO's response to hybrid threats Last updated: 08 Aug. 2019, Retrieved from https://www.nato.int/cps/en/natohq/topics_156338.htm

Nepal Corruption Rank, Trading economics Retrieved from https://tradingeconomics.com/nepal/corruption-rank

Sandor, F., *Hybrid warfare revisited,* Retrieved from https://globalecco.org/hybrid-warfare revisited

Sehgal, I. (2018). *Understanding hybrid warfare*, Retrieved from http://southasianmonitor.com/z column/understanding-hybrid-warfare/

Summary of the 2018, National defense strategy of the United States of America; Sharpening the American military's competitive edge p. 4 web https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy Summary.pdf

TRADOC Pamphlet 525-3-1; *The U.S. Army operating concept: Win in a complex world* 2020-2040, 31 October 2014

UK's National security strategy and strategic defence and security review. (2015). Retrieved from https://www.gov.uk/government/publications/national-security-strategy-and strategic-defence-and security -review 2015 and https://www.nato.int/cps/en/natohq/offical_texts_156624htm