Deterrence in the Age of Hybrid Threats

Amit Gaur*

Warfare has constantly evolved to match the environment. In the contemporary era, borders are not only territorial but expand into the social, economic and cognitive domain as well. Warfare has also graduated to utilising every possible means in its quest to find more ways to meet the ends. As strategy evolves to use every possible tool across domains by posing hybrid threats, strategy to counter such attempts also takes shape by recalibrating their approach towards deterring adversary from employing such threats. Achieving deterrence is the first step in countering hybrid threats but not with the same outlook with which Conventional or Nuclear Deterrence is conceived. This commentary attempts to highlight the need for adopting a deterrence strategy designed to overcome hybrid design of emerging threats.

Hybrid Warfare: A Cocktail of Lines of Warfare

Conventional or regular warfare largely aims to violate physical boundary in a state versus state conflict, whereas irregular warfare targets political, cyber, space, cognitive and many other such domains. A few of these domains overlap with the military domain while some do not come under the mandate of armed forces. Vulnerabilities present across these domains can be targeted linearly, more so when they are conducted in isolation and more importantly

* Wing Commander Amit Gaur is a Research Fellow at Takshashila Institution, Bengaluru, India.

ISSN 0976-1004 (print); 2583-7567 (online)

Journal of Defence Studies, Vol. 18, No. 2, April–June 2024, pp. 128–137

with denied attribution. For example, attack on power grid or terrorist attack by non-state actors. When a number of such vulnerabilities are targeted near simultaneously or coupled with conventional means, it takes the shape of hybrid warfare, which is evidently an intrinsic element of modern conflicts. These domains and thereby irregular instruments of warfare get shaped from evolving social, political and technological environment and vulnerabilities therein get exploited owing to disruptive technologies or innovative use of existing technologies.

The strategy to identify and target these vulnerabilities has evolved to suit the needs of an actor to challenge otherwise more powerful but status quo states as part of irregular warfare. However, modern warfare relies on the fusion of irregular and conventional (regular) strategy, aptly called hybrid warfare to expand battlefield domains ranging from physical to cognitive while aiming to exploit maximum.

Sean Monaghan in his paper, 'Countering Hybrid Warfare' denotes any identified vulnerabilities inherent to these domains as hybrid threats, a term first coined by Frank Hoffman, a former US Marine and a defence scholar in 2007. Sean depicts a spectrum of lines of warfare as per their intensity and probability of occurrence (Figure 1).

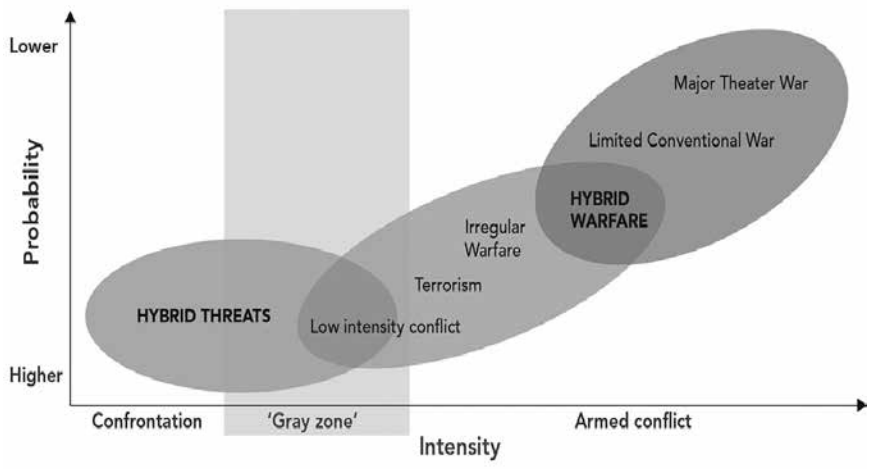

Figure 1 Hybrid Threats on a Continuum of Conflict

Source: Monaghan Sean, 'Countering Hybrid Warfare: So What for the Joint Force?', *PRISM*, Vol. 8, No. 2, October 2019, available at https://ndupress.ndu.edu/PRISM/PRISM-8-2/, accessed on 1 December 2023.

Hybrid Threats

To understand the onset of conflict involving hybrid threats and line of hybrid warfare, it will be prudent to look at the relations between two states through the broad lens of 4Cs under the ambit of Peace and War.

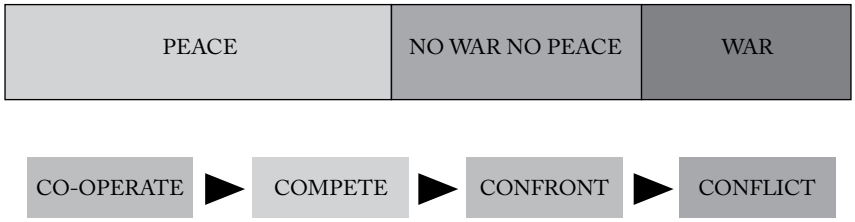

Figure 2 Stages of Interstate Relations
Source: Created by the author.

Hybrid threats manifest in the environment of 'No War No Peace' marked by confrontation across domains, both seen or unseen or termed as kinetic or non-kinetic ones. When two entities' self-interests intersect beyond their own belief of righteousness, competition transforms into confrontation. It is seen not necessarily in the domain they were earlier competing in but in other domains. Confrontation breeds hybrid threats out of inherent vulnerabilities. These threats and their efficacy are not new and being repeatedly seen earlier in the form of indirect approach, or Sun Tzu's *winning without fighting* strategy. Their recent widespread blending with conventional warfare makes them more lethal. The more the battlefield becomes inclusive and interdependent on variety of domains, the more complex approach will need to be evolved to fight it.

Ultimately, War is War. Clausewitz told us that war is more than a chameleon and revolves around the paradoxical trinity of People (Chance), Military (Violence) and the Government (Political considerations). However, history tells us that *warfare* is definitely a chameleon, which adapts most suitably to the prevailing environment in which war is being fought to optimise the outcome with given effort. If conventional warfare has been traditionally known to be targeting the military and government part of Trinity, Irregular warfare focuses more on the People and Government. However, hybrid warfare has the ability to affect each facet of everyday life across domains; targeting People, Military and Government in a non-linear fashion.

Waging, Countering or Surviving Hybrid warfare begins at understanding hybrid threats even before they could bear effect. As domains in which threats are being posed are not exclusive to military, exploiting them against an adversary or countering them will require a whole of government approach. The four pillars on which formation and execution of Hybrid threats rest can be thought of as:

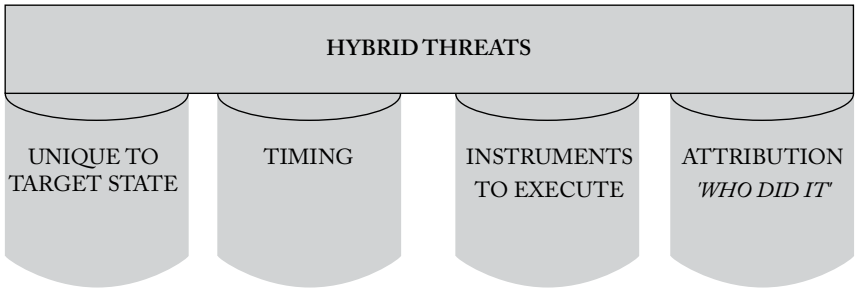

Figure 3 Pillars of Hybrid Threats
Source: Created by the author.

There is no Hybrid threat master plan universally applicable. Domain vulnerabilities may be constant but targeting them will not give the same results for every state. The target state has to be studied in detail to identify the vulnerabilities that are unique to it and then target them. It is designed for the target state for maximum efficacy.

The omnipresent vulnerabilities in Social, Religious, Political, Cognitive and Emerging technological domains are best exploited when their timing is managed effectively to use the environment most optimally. For example, exploiting religious fault-lines can produce more effect during festivities rather than on Independence Day celebrations. Infusing a political turmoil in the target state when it is at the cusp of economic boom and prosperity will hurt the state more. Also, the varieties of options available ensure that actions remain below the international and domestic threshold of conflict and yet achieve results by weaponising everything present in our lives.[1]

Having identified the target, next is the selection of instrument for execution. Whether to employ a financial, military, psychological or ideological/religious instrument is the choice deduced from this strategy.

Attribution can be the biggest strength of hybrid threats. An option may not mandatorily be exercised every time, however it enables preparatory side to bypass legal frameworks of conflicts as and when desired.

Deterrence: Present and Future Trajectory

Deterrence, in its broadest sense, means persuading an opponent to not initiate a specific action because the perceived benefits do not justify the estimated costs and risks. The classical understanding of 'Deterrence' has three factors: *Capability, Credibility and Communication*, that is, ability or capacity to implement deterrent measure and the will to implement and communicate cost-benefit analysis for both sides.[2]

Sean argues that the rise of hybrid threats can be traced to both successes and failures of deterrence. On the one hand, deterrence has often succeeded in dissuading revisionist actors from resorting to conventional armed aggression. Yet, at the same time it has often failed to dissuade those actors from conducting hostile state activities in the form of hybrid threats.[3]

The existing approach of deterrence revolves around conventional and nuclear deterrence. These take into account specific threat types, accepted thresholds and response mechanism. This may not be ideal for countering hybrid threats in the low intensity phase of irregular warfare or even in high intensity hybrid warfare itself as threats and their associated thresholds and suggested response mechanism are as complex as the hybrid threats and warfare itself. Prevalence, ambiguity and attribution necessitate relooking the approach to fulfil the requirement of three 'C's of Deterrence.

Relooking Deterrence in a Hybrid Environment

If state has to prepare a deterrence strategy against hybrid threats, it should re-approach every 'C' of it. The aspects of capability building that need to be factored in for emerging threats remains the very first step of deterrence in present times. Approach to build conventional capability and capacity is successful for threats that can be neutralised through them. But threats which do not challenge such capabilities and remain below the threshold of their response mechanism necessitate developing resilient strategy through timely preparation. From purely defensive perspective, ability to predict emergence of these threats relies on honest and comprehensive introspection of own vulnerabilities as part of preparation. Intelligence is the bedrock of this step. Many such vulnerabilities lie outside the military domain and require all of government approach. Gone is the era when an attack would typically mean violation of your territorial borders. Today, every possible line of national, social and personal space is a border needing to be defended. Even after detecting such threats, prevention for their manifestation on ground calls for a proactive approach by targeting 'ways' of adversary.

Accumulation of these approaches is to prevail against threats. To this to succeed; Preparation, Prediction and Prevention lies across all the elements of national power. Will to implement counter-measures or *credibility emanates* from a thorough understanding of the details of threats and accepting it as a cross-domain responsibility and form a joint response. Prevailing against hybrid threats requires strategy, which is also hybrid in its composition and not one domain (military, diplomacy or society) centric. Due to a lack of attribution, communication is a challenge but has to be achieved through capability demonstration as and when required.

Pillars of Hybrid Deterrence

An approach that can be useful in adopting deterrence strategy against hybrid threats is that of strengthening one's own system. It adopts a four-pronged inward-looking approach. It aims at developing all-round capabilities for the present and future and not for a bygone era (Prepare), to develop an ecosystem which can foresee their emergence (Predict), if emergence does take place, Prevent their realisation or restrict their impact and in the end employ hybrid solution to Prevail over hybrid threats.

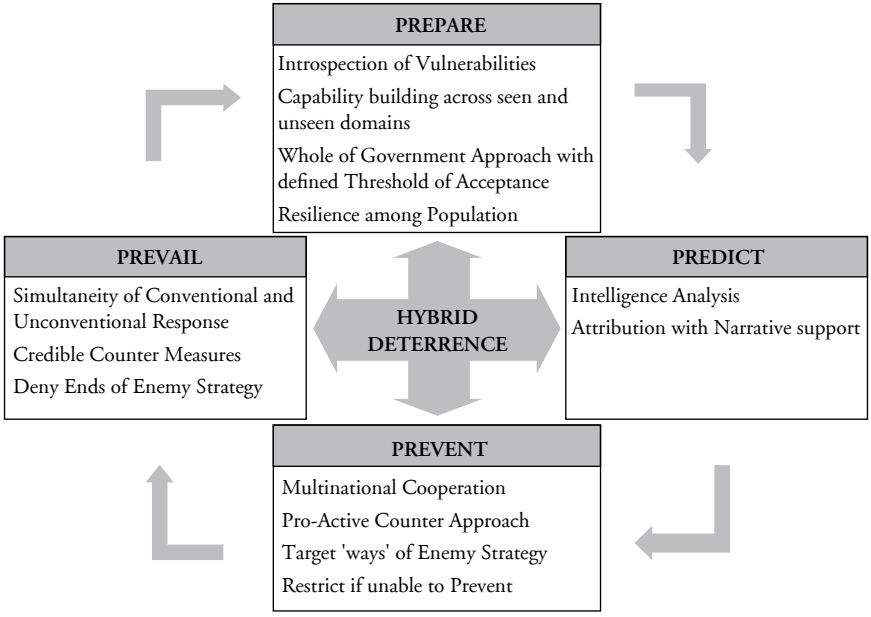

Figure 4 Four Pillars (Ps) of Hybrid Deterrence
Source: Created by the author.

Prepare

Capability-building is a process with a definite function of time. A capability not acquired in time will not the serve the purpose of acquiring it. A comprehensive appreciation of own vulnerabilities will propel to seek mitigating capabilities. Functional dependency of assets across domains requires capability development across domains. A capability enhancement in Air, Naval or Land domain in terms of conventional approach may fall short if not matched by Cyber or Space. Today, approaching a hybrid problem necessitates a hybrid solution. It is possible by working out a comprehensive solution and not getting trapped in domain-specific approaches. Coordination among all elements of national power not only at planning or operating level but right from the beginning when presenting their capability seeking long-term perspective plans is the only way forward.

An important aspect of any warfare is people. A part of Clausewitz's trinity holds a lot in balance when it comes to something like countering hybrid threats. After World War II not on many occasions, the will and resilience of people has been tested. As target of hybrid threats includes government, military and people, an effort has to go into preparing people to fight against such threats and develop tolerance against them. Probably, required approach can be more aptly termed as *whole of society or nation approach,* a term getting traction in recent times.

Defining a threshold for a reactive mechanism against a hybrid threat is easier said than done. However, for any successful deterrence strategy, this has to be considered without compromising on necessary strategic ambiguity. Though the scale of reaction can be kept *ambiguous,* the *communication* of intent will get a boost if such threshold can be defined.

To counter the target-specific design of hybrid threats, constant learning and re-learning of self and adversary is required to seek and attain right capabilities at the right time. All in all, a well-prepared outlook to understand the intricacies of threats and efforts to address them will counter-balance hybrid threats.

Predict

No single intelligence source or organisation can warn against such threats. Actors or instruments of choice constantly changes here. Information overload is certain. Still the situation warrants that an analysis of existing intelligence must look into the aspects which may seem mundane in isolation

however have a profound effect when seen though the perspective of hybrid threats when fused together. It will also help in identifying vulnerabilities and to predict exploitation of them. This may also be useful in identifying the preferred instruments by the adversary.

Another strength of hybrid threats is lack of attribution. If intelligence can mitigate this challenge, it may deter the use of threats being posed on the basis of deniability. Accurate and timely attribution can itself act as deterrence at times.

Prevent

The core of prevention lies in targeting the adversary's 'ways' or instrument of choice. Addressing them proactively through own means or multinational cooperation can be useful in preventing the onset of hybrid threats. For example, blacklisting terror organisations, ceasing their funding and finances can cripple the choice of using non-state actors against the adversary.

Vulnerabilities and associated hybrid threats are omnipresent in every domain of life. It makes 100 per cent prevention of such attacks impracticable. So, the measures to restrict their impact in severity and occurrence are equally important by developing redundancies. For example, restricting the impact of cyber-attacks is far more practicable than preventing it completely. In many such domains, preventing and restricting are complementary to each other and must be supported by redundancies in each domain.

Internal security is the lynchpin of successfully implementing this step. The modernisation of internal security agencies incorporating technological advancements can help in creating important practical tools to combat the adversary's 'ways'.

Prevail

In the face of hybrid threats, blending of response is the only way to counter them. If 'ways' of adversary could not be targeted earlier, it is essential to not let his 'ends' go out of sight while countering threats. Resolute but calibrated response is essential to add credibility to the response mechanism. The problem is how to design a response mechanism against a threat which itself was uniquely designed against the state. The answer lies in fighting at every targeted level coherently and rely on redundancies. Even the most inconsequential looking link in the system has a role to play. But for that link to react in a desired manner, it should be brought into a structured response

mechanism. This can be achieved through an organisational structure encompassing all ministries and creating awareness.

The Way Forward

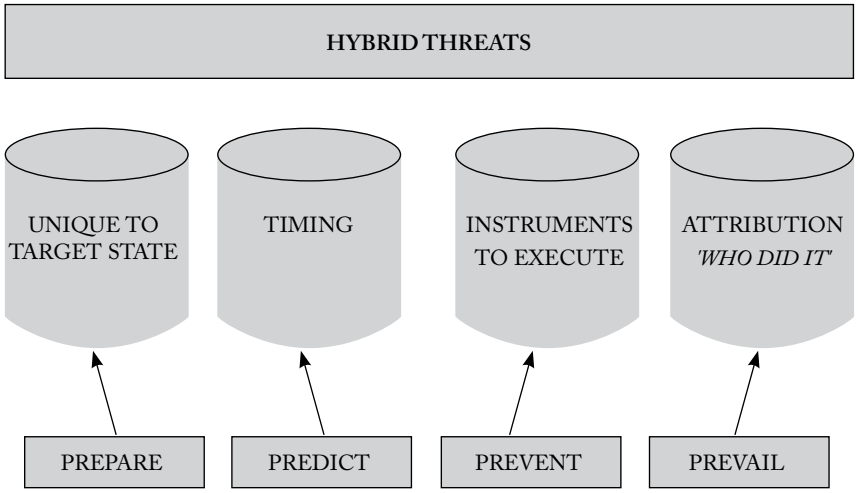

Figure 5 Mitigating Hybrid Threats
Source: Created by the author.

Capability, Communication and Credibility remain the most potent theoretical guidance to achieve deterrence, be it conventional, nuclear or hybrid. As warfare is including more and more 'ways' to use all available 'means', countering them also requires rethinking in terms of capability development plans, redefining thresholds of acceptance and the legal definition of war itself. Every aspect of social, economic and technological environment presents variety of 'means' to adversary to exploit. Deterring adversary, in adopting this approach, mandates fortifying these aspects to minimise exploitation and have redundancies in place. Each of these aspects falls under different instruments of national power. A coherent deterrence strategy that aims to strengthen one's own house, has the potential to weaken the pillars over which the foundation of hybrid threats rests.

Notes

1. Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, Yale University Press, 2022.

2. Robert P. Haffa Jr, 'The Future of Conventional Deterrence: Strategies for Great Power Competition', *Strategic Studies Quarterly,* Vol. 12, No. 4, Winter 2018, pp. 96–97.
3. Sean Morgan, 'Deterring Hybrid Threats', The European Centre of Excellence for Countering Hybrid Threats, available at https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/, accessed on 25 November 2023.