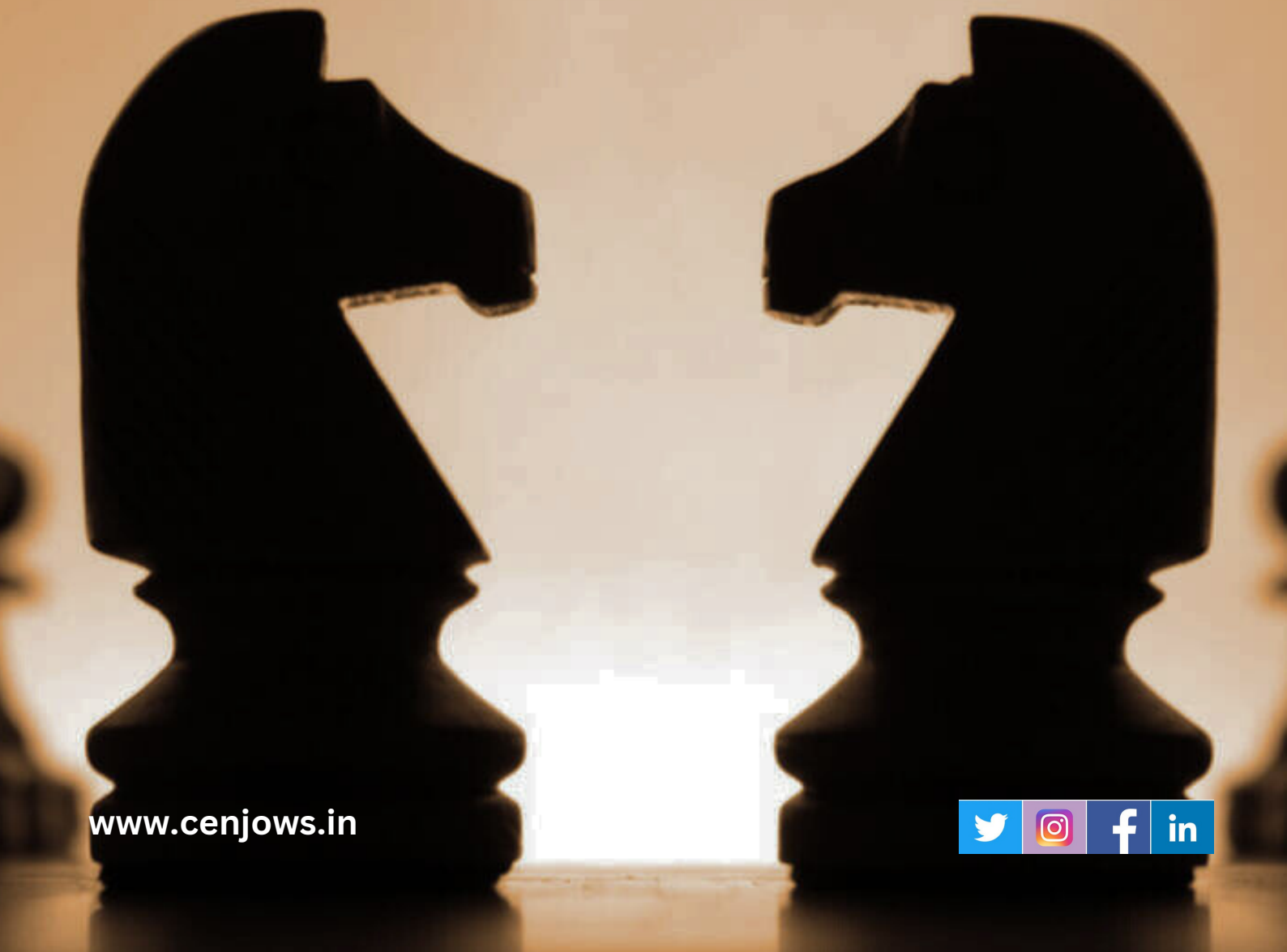
CENJOWS

ISSUE BRIEF
IB/04/24

DETERRENCE IN THE 21ST CENTURY NEEDS A STRATEGIC RECONSTRUCT

LT GEN AB SHIVANE, PVSM, AVSM, VSM (RETD)



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

DETERRENCE IN THE 21ST CENTURY NEEDS A STRATEGIC RECONSTRUCT

Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd) is the former DG Mechanised Forces and a Strike Corps Commander. The Officer is a defence analyst and prolife writer on matters military. Presently, he is Distinguished Fellow and COAS Chair of Excellence at CLAWS.

Abstract

This paper discusses the 21st-century evolving deterrence landscape arguing for a strategic reconstruct. It focuses on challenges presented by non-state actors, technological change and evolving geopolitical structures. By looking at scenarios such as the Russian-Ukraine War and Israel's deterrence approaches, it analyses contemporary deterrence's intricacies and evolving challenges. The paper proposes the concept of integrated deterrence with a focus on cross-domain capabilities and adaptive approaches specific to each adversary. It recommends the deterrence construct moving from a "cost-benefit" model to a "risk-consequence" model. The paper dispassionately analyses the present shortcomings of the Indian deterrence strategy and recommends imperatives for adding teeth to it. The recommendations range from vitalising national security policies to strengthening military capability and cyber deterrence.

Keywords: Deterrence, Kinetic and Non-kinetic Threats, Nuclear, Information Age, NATO, Russia-Ukraine War, Cyber and Non-state Actors

Introduction

Deterrence, as a strategic concept, has roots deeply embedded in the ancient historical past going back many centuries. Recorded historical highlights that deterrence existed between adversarial states by showcasing military power and credibility of action. Deterrence evolved in the Cold War era gained credence as an essentially state-

centric model with nuclear brinkmanship.[1] It prevented full-fledged conflict in a bipolar world, yet escalated competition with technology creating new domains of warfare.

In the 21st century's geopolitical volatility, traditional ideas of deterrence face unprecedented challenges from emerging nonstate actors and new domains of war. The ongoing wars particularly Russia-Ukraine and Israel Hamas have once again proved the fragility of legacy deterrence. In Asia too, the Chinese Himalayan transgression and forays into the sea, Pakistan's proxy war in J&K and Iran-Pakistan's recent cross-border aerial strikes have tested deterrence though kept it below a conflict threshold. Thus, deterrence construct that is solely focused on nuclear arms or legacy conventional conflict is no longer sufficient for limiting aggression by an irate adversary, especially below the conventional threshold.

Former NATO Deputy Secretary General Vershbow commenting on deterrence in the 21st Century stated: *"It requires effective, survivable capabilities and a declaratory posture that leave the adversary in no doubt that it will lose more than it will gain from aggression, whether it is a short-warning conventional attack, nuclear first use to deescalate a conventional conflict, a cyber-attack on critical infrastructure, or a hybrid campaign to destabilize allies' societies."*

India's deterrence posture needs reconsideration in light of the 21st-century dynamic operational environment and be expanded to include sub-conventional domains both kinetic and non-kinetic. Further, it must address the challenges of deterring Information Warfare and cyber-attacks.[2] Deterrence reconstruct strategies to these evolving dynamics requires innovative thinking, doctrinal review and multidomain capability building to an operational matrix defined by complex multidomain threats.

Deterrence Paradox in the 21st Century

- **Changing Character of Conflict**

  While the nature of war is persistent, its character is ever dynamic and evolving. The contemporary landscape of security is marked by a shift from traditional state-on-state warfare to multidomain, asymmetric threats both kinetic and non-kinetic. The landscape is increasingly marked by non-state actors, proxy tools and lethal multi-domain technology, which has blurred the line between war and peace. The non-state actors from transnational entities to hacktivists have emerged as formidable players in the world platform adding complexity to the deterrence construct.

  This shift threatens traditional deterrence mechanisms, clearly designed with nation-states in mind and often centred on the prospect of overwhelming military retaliation. With their shadowy structures and abnormally out-of-the-ordinary strategies, non-state actors render these traditional models woefully inadequate.

In the words of Dr Mary Kaldor Professor of Global Governance, at the London School of Economics, *"The traditional idea for deterrence always assumes a rational actor that is properly guided from within. Non-state actors work with other sets and rules hence making it difficult to enforce normalcy in them."*

- **Technological Advancements and New Domains of Conflict**

The 21st century has witnessed technological changes and disruption in all sectors as the norm today. The evolution, proliferation, and combination of technologies, are challenging the effectiveness of deterrence especially with globalisation leading to geo-technology. The contact and non-contact warfare dimensions have reached new milestones, which have greatly influenced the deterrence construct. Autonomous fighting platforms, cyber warfare and Unmanned Aerial Vehicles / Drones have already begun to impact warfighting strategies. Directed Energy Weapons, Nano Technology, Quantum Computing, Big Data Analysis, the Internet of Things and Artificial Intelligence will have a transformational impact on the planning and conduct of warfare and will revolutionise traditional notions of deterrence.

Such disruptive technologies give both state and non-state actors the ability to bring new dimensions to the threat matrix beyond the traditional lines. These technological spheres challenge the efficiency of traditional deterrence because they are interconnected. Dr. William J. Perry, Former U S Secretary of Defence, emphatically states, "*In the cyberspace age the conventional idea behind deterrence due to threats provoked by enormous retaliation is turning outdated the harm caused in cyberspace might not necessarily demand such magnitude response as traditional military or armed conflict does".*

- **Multipolar World Order**

The world continues to evolve in its transition toward a more multipolar order where the power centres are diverse and alliances continue to shift. Traditional models of deterrence inherent in the bipolar or unipolar paradigms that once prevailed, face challenges in a world that is becoming more multipolar with the rise of new powers and power diffusion among states. This reality of a globalised world adds a new dimension to the actions of both conventional and non-conventional threats with added ambiguity and complexity. In the words of Dr Anne Marie Slaughter, President and CEO of New America, *"In a multipolar world where power is distributed among multiple actors inherently deterrence becomes about influence persuasion strategic alignment as much or more than the traditional threat of force."*

- **Nuclear Deterrence Challenges**

Nuclear deterrence in the erstwhile nuclear global order of a bipolar world had stood the test of time. However, with multipolarity, new actors in battle space and emerging technologies its effectiveness is being questioned as a war preventive

strategy.[3] Former Indian National Security Advisor Shivshankar Menon says, *"The nuclear age no longer belongs to a few major powers alone; the rise of regional nuclear states and possibility for non-state actors acquiring these devastating weapons also bring about complications that cannot be handled smoothly by traditional deterrence models."* Nuclear weapons thus slipping into the hands of non-state actors added an unforeseen dimension, fraught with possible proliferation and global risks, particularly from fragile or radicalised states like Pakistan.

- **Erosion of Credibility in an Information Age**

In an age when information rapidly flows, the legitimacy of deterrence is under severe stress. Credibility is often shaped by scripted narratives and perceptions as part of an information campaign. Credibility and plausibility with demonstrated will are thus two sides of the same coin.

In an information age, the dynamics of credibility change and thus reshape the field in which deterrence strategies function. As Dr Kathleen J, McInnis writes as a Specialist in International Security at the Congressional Research Service *"States must now operate within the information environment where public opinion and global scrutiny along with narratives propagated by both state or non-state actors play an important role towards determines that if deterrence of war strategies will fail or succeed"*

India needs to invest much more in winning the war of narratives and favourably swinging perceptions to its advantage. Ironically in Kargil 1999, Balakot Surgical Strikes 2019 and Galwan Clashes 2020, despite the bold and brave actions, the war in the information space was lost by India. In future deterrence policies where war has become an integral part of society, winning the information space is as critical as deterring the war and if undeterred winning the war.

- **Economic Interdependence and Non-State Actors**

The increased interdependence of global economies has created a new aspect of deterrence. Non-state actors with economic power and the ability to exploit interdependent financial systems can bring pressure that goes beyond what we are used to seeing coming from military strength. Economic interdependence has made traditional military solutions unattractive. Non–state actors recognise these vulnerabilities in the modern economy and use them to achieve their objectives. A recent example has been the Houthi attacks in the Red Sea and the Hamas terrorist attack on 7 Oct 2023.

Further, in contemporary conflicts, the economic toolkit is as crucial for statecraft as the military one. Non-state actors and proxy states, especially those that possess economic resources can use these tools to accomplish strategic goals without the need for conventional armed forces.

Deterrence Reconstruct: Navigating Challenges

Three key elements are significant to the deterrence construct: one, the perception of the capability of the force and potency of the weapon, two, the perception of will and its communication, and three, the perception of the credibility and ability to implement intentions.[4] The challenge remains their multidomain and cross-domain linkages. Strategic deterrence policies should extend across the entire threat spectrum posed by potential adversaries, rogue states, and non-state actors. While non-state actors currently present the greatest immediate threat, the focus should not be myopic addressing the effects, but a long-term approach to address the roots and prevent undesirable actions.

Deterrence must be context-specific, considering the military, political, social and cultural characteristics of each specific adversary. Any ambiguity indicating ineffective policies and insufficient investments could potentially lead to failed strategies. A lucid and holistic deterrence strategy tailored to each threat environment, utilising all instruments of power, is thus essential. Thus, deterrence construct must identify suitable instruments to assess an adversary's behaviour and communicate plausibly.

Similarly identifying the fundamentalist ideology, culture, motivation and objectives of non-state actors can facilitate developing deterrence policies against such threats. Yet these are often beyond the conventional construct of deterrence policies and require a more innovative and ingenious outlook with enhanced dynamism. Proxy wars as seen in contemporary times and rogue regimes offer new challenges to legacy deterrence mandating a unique framework.

Cyber-attacks and cyber terrorism are modern tools of non-kinetic threats to a nation. Their prevalence in a peace-war continuum acts as silent killers. Deterring these attacks becomes paramount. Coordinated interagency collaboration and a profound understanding of cyber threats with indigenous technology interface are crucial to developing effective cyber deterrent policies.

However, deterrence is not foolproof, and its failure can be attributed to factors such as bounded rationality, a credibility gap between capability and will, ambiguity in policy, and the failure of the strong to deter the weak. To reduce deterrence failures, effective communication, understanding adversaries, and credible policies are essential. Yet nations need to be prepared for eventualities of deterrence failure.

Deterrence and Risk Proclivity

In deterrence dynamics, deterrence and risk are two sides of a coin, shaping the contours of strategic decision-making. Deterrence risk propensity and management define the different stances towards risk that an opponent could inflict and direct the challenges associated with deterring, dissuading, and/or defeating threats.

At the heart of deterrence strategies is risk-proclivity which can be described as a risk scale between two extremes-risk tolerance and risk avoidance, with relative probability versus anticipated value balanced against possible enemy reactions. Despite the thin line between risk and danger, actors' actions in navigating this dynamic association are perceptible.

When the chance of undesired escalation exceeds the expected value of an action, risk aversion holds on actors. Yet, as the chances of controlling the levers of escalation to advantage emerge, a risk-taking propensity appears which reflects the dialectics behind deterrence and risks in this complicated network. This analytical narrative makes strategic intelligence and informed risk management critical for minimizing potential risks. This governs the foundation of deterrence philosophy leading to the study of the risk-consequence model as an alternative.

Cost-Benefit to a Risk-Consequence Model

Deterrence largely depends on an adversary's assessment of the "cost and benefit" of his plan, wherein the benefit outweighs the accrued cost, of his intended actions. However, the correlation between the intended costs and perceived benefits being ambiguous merits consideration of a more holistic "risk and consequence" model.[5] This model aims as part of the deterrence strategy to give a more pragmatic direction of 'methods and means' to choose for deterrence.

The legacy Cold War cost-benefit model remains fragile against an autocratic regime and new domains of threats like non-state actors, with attendant irrationalities and ambiguities. The irony of Pakistan's political fragility, puppeteer to the military and mullahs, and China's Xi-led autocratic dictatorial regime make the cost-benefit model even more perilous with collusive bonhomie adding another dynamic. Thus deterrence construct for India's hostile and revisionist cultural neighbours needs to be considered differently. Deterrence by threatening war escalation may not be desirable for the larger national interest. Thus, deterrence based on controlling risks and managing consequences, could be a more pragmatic model. Yet, deterrence, against India's revisionist neighbours, can never be guaranteed and thus the nation needs to be prepared for the escalation ladder with indigenous capabilities.

Deterrence to Integrated Deterrence

Integrated deterrence demands a nuanced and tailored strategy, specifically calibrated to address diverse adversaries and scenarios, while navigating the complexities of unique political circumstances. It requires a sophisticated blend of technology, operational concepts, and capabilities intricately interwoven in a networked fashion for strong communication. [6]This amalgamation must be so inherently credible, flexible, and formidable that any potential adversary is compelled to reconsider their actions. The goal is to establish advantages for ourselves and create strategic dilemmas for the adversary.

The concept of integrated deterrence is characterised by three distinctive features. Firstly, it is inherently cross-domain[7] and universal, aiming to deter all forms of security threats through the utilisation of all available means. Secondly, it is seamless and ever-active, operating both in peace, war and post-conflict including hybrid grey zone situations. Thirdly and more critically, it has a vertical as well as a horizontal escalation constituent integrated with levers of control firmly gripped.

Achieving an integrated deterrence includes a calibrated reimagining of the existing capabilities, the adoption of creative operational concepts, and investments in indigenous cutting-edge technologies like quantum computing for the future. It must have a multidimensional array of military and non-military competencies. This integration constitutes the posture of "integrated deterrence," essential for safeguarding national security. The challenge lies in going beyond the strategic level and comprehensively applying deterrence in situations below the conflict threshold.

Importantly, integrated deterrence is characterised by integration across all conventional, nuclear, cyber, space, and informational domains. This integration addresses all theatres of competition and likely conflict, across the entire spectrum from conflict including the ambiguous grey zone. The concept further involves the assimilation of all instruments of national power and security, including forging global partnerships.

In essence, achieving integrated deterrence demands an inclusive and holistic approach that optimises the full spectrum of capabilities, surpassing traditional boundaries and adopting innovation and collaboration through strategic partnerships.

Deterrence in the Russian–Ukraine War

The Russian-Ukraine War is a case study of 21st-century deterrence dynamics. It has shown the short-sightedness of the Western deterrence construct and dissuasion dynamics. The threshold of tolerance was neither envisaged nor a pre-emptive strategy evolved to dissuade such an eventuality.[8] The incremental strategy of NATOfication and looming threats to Russia resulted in deterrence failure and Russification of Ukraine which became a pawn in the Western strategic chess board. The war highlights the need to comprehend an adversary’s strategic tolerance and motives linked with typical deterrence against a committed actor seeking its geopolitical goals and challenges.

Sanctions too are an abject failure as tools of deterrence. Sanctions don’t change nation-states' behaviour but have an adverse ripple effect on global stability, particularly in the third-world economy. Sanctions rather than creating regional stability create global instability by denial regimes and global economic crises. As seen in the Russia-Ukraine war, sanctions have failed as instruments of effective deterrence.

Israel's Deterrence Conundrum

The Israeli deterrence strategy of *'mowing the lawn'* showed its limits much like the much-hyped *'surgical strikes'* in the Indian context in dealing with cross-border terrorism. Recent events like the 7 October barbaric attacks by Hamas have highlighted weaknesses in a simply punitive approach and emphasised that a more comprehensive, all-encompassing strategy involving diplomatic measures as well as trading political situations is needed to create long-term stability in the region.[9] It has raised the importance of a comprehensive integrated deterrence. Further, it has highlighted deterrence may be temporal and its evolving dynamics would show cracks which need to be plugged periodically.

The recent Iran-Israel shadow wars coming to the front by missile and drone strikes again bring out the new dimension of deterrence and the notion of victory through wars of narrative. Finally, prudence states that while deterrence works, its failure must not be a surprise for military responses or breed complacency.

Indian Deterrence Strategy: Need for a Review

Ironically, Indian deterrence has only partially stood its ground though kept the threshold below full-fledged conflict.[10] Thus both China and Pakistan exploit ambiguity and India's risk aversion as part of their sub-conventional strategies. Added to it are nonstate actors, cyberspace and information space challenges. An odd surgical strike does not bury the ghosts of Kargil or Galwan. Nuclear deterrence between India and its nuclear neighbours has diminished the likelihood of an all-out conflict but has enhanced the threat of skirmishes and standoffs below the conflict threshold. [11]Yet these could brew a larger storm with added unpredictability.

Doctrinally, the present deterrence strategy needs a review to have more teeth, better integration, greater expanse and visible effect. Effective deterrence in the 21st century will need a specific strategy for each actor to be deterred. This would require a whole of nation approach to evolve cohesive deterrence policies based on an adversary's strategic culture, motives, rationale, risk profile and perceived vulnerabilities.

India's approach to deterrence remains risk-averse to dissuade a major power like China. Its aim to deter China failed possibly due to capability differential, which in turn rendered its deterrence construct vulnerable resulting in Galwan. Yet its deterrence averts a conventional war for three reasons. One power differential is not adequate for China to achieve its objectives, two both are nuclear states and three, China's primary focus lies on Taiwan and threats in the Indo-Pacific. India remains an irritant to China in its regional primacy and global stature.

India has made the considered decision not to escalate border tensions to war. Ironically, its deterrence measures failed to curb border skirmishes and intrusions resulting in the status quo being altered.[12] The "cost-benefit" of escalation does not auger well, more so at a time when India's global trajectory is on the rise and much

needs to be done to bridge the power differential between the two nations. Yet the future burgeoning threat from China and its collusion with forces inimical to national security must not be ignored.

The traditional manner to deter an adversary is based on a negative cost-benefit model for the adversary. But such a deterrence construct often remains ambiguous and perceptions may differ. Conversely, a risk-tolerant model dissuades an adversary by increasing the perception that his action would not achieve the desired objective and embarrass him with the certainty of retribution. This model would be favourable for Pakistan but not necessarily for China presently, purely on capability and credibility terms, which makes deterrence communication non-plausible. Thus Pakistan is suited for a risk-tolerant model, while China is suited for a risk-averse model reinforced by a risk transfer collaboration through strategic global partnerships and multidomain capabilities especially on the oceanic front.

The deterrence risk tolerant strategy against Pakistan must thus rely on punitive deterrence, with an inbuilt pre-emptive denial strategy against any possible misadventure. Punitive deterrence is defined as a policy of assured retribution with demonstrated capabilities imposing severe punishment on an opponent while controlling the escalation ladder and being prepared for responses.

Against China the dynamics and power differential are different. Thus a risk-averse deterrence construct against China finds favour while bridging infrastructure and capability gaps. Such an approach aims to minimise the risk of war unless forced upon. Yet it also assures the adversary's denial of his aims through a calibrated risk-consequence construct based on controlling risks and managing consequences. In such cases, deterrence must yield to deterrence by denial. Denial is pre-emptive and proactive which aims at increasing the likelihood of an opponent’s strategic objective failing. If pre-emption fails then it is a quid-pro-quo capability to dislocate the adversary. Such a model of risk-averse deterrence by denial cum domination complemented by risk transfer caveats would work well against China till asymmetries are removed.

Admittedly, China was not deterred from risking its incursion and salami-slicing strategy. However, it has been dissuaded from escalating the threshold to conventional conflict. Indian deterrence by denial cum domination must aim to “restrain,” “keep out,” or “hold back” China. Indian deterrence against Pakistan by punishment, must aim to punish its terror handlers both by overt and covert actions while escalating the cost of proxy war both vertically and laterally. Both these require managing the international environment as conflict is no longer just about two adversaries.

Till a power differential remains, India will have to manage its risk, by narrowing the capability gaps as a priority thereby raising the risk for China to cross threshold levels. Till gaps exist a risk transfer model would additionally help in creating ambiguities adding to deterrence. Risk transfer can occur through collaborative global partnerships, such as QUAD and joint military training. It thus enhances China’s probability of failure to achieve its strategic aims, through countervailing strategic partnerships and military

cooperation with nations averse to Chinese belligerence. The combined economic and indirect military might of nations could deter China, due to the consequences of reducing its global power status, and political standing or by an adverse impact on its economic trajectory. Further, the risk of war could create vulnerabilities to its strategic global stature and ambitions.

Strengthening the India's Deterrence Posture: Imperatives

1. National Security Strategy (NSS): A well-defined national security strategy is imperative for a plausible deterrence. It must unequivocally state the threats, desired capabilities and deterrence construct with clarity of capabilities, credibility of intent and explicit communication. This strategy should be dynamic, adaptable, and all-encompassing, involving all stakeholders contributing to national security. It must cover the entire spectrum of multidomain threats in an integrated manner. NSS is foundational to convey the intent and strategically communicate the responses for deterrence to be plausible.

2. **Strengthen Collective Security Mechanisms:** India must strengthen collective security and defence technology partnerships, especially in the face of common state and non-state actor threats including terrorism and cyber-attacks for a risk-shared and collective response mechanism. Collective security mechanisms facilitate deterrence by a sharing approach which ways in the mind of the adversary.

3. Atmanirbharta and Defence Industrial Base: Investment in self-reliance and self-sufficiency with a focus on indigenous technology infusion is critical. Testing war stamina during peacetime by evaluating the defence industry surge capabilities and reserve stocks is critical. Indigenous capabilities contribute to the risk and consequences model.

4. Integrated Deterrence: Building a robust deterrence strategy requires leveraging all instruments of national power including technology, cyber, diplomacy and economic power besides military. These must be intricately woven together across all domains of warfare. This integration would span the entire spectrum of conflict including the ambiguous grey zone and includes cross-domain deterrence. The concept further involves the assimilation of all instruments of national power and forging global partnerships.

5. Adaptive Deterrence Strategies: Transformative deterrence strategies should be reviewed and adapted to dovetail non-traditional threats and modern tools of powerplay. A blend of hard power and soft power is essential for effective deterrence. A risk-tolerant deterrence by punishment model for Pakistan and a risk-averse deterrence by denial cum domination model for China, supplemented by risk-sharing partnerships need deliberations.

6. Military Transformation and Joint Force Restructuring: Military transformation to be sustainable must address all three critical components; transformed politico-military

culture, transformed defence planning process and transformed joint service capabilities. Future-ready Army must be a budget-supported transformation plan that prioritises people and balances operational readiness (a combination of operational preparedness and operational effectiveness), with doctrinal reconstruction, joint force restructuring, modular lean and agile forces, modernisation, and reoriented professional military education. 'Integrated Joint Theatre Command' is indeed the destination but the path must be trodden by first strengthening desired capabilities and jointness of professional military education. The need is to build tri-service capabilities beyond a single-service parochial approach based on a joint military strategy and tri-service culture to achieve desired political objectives.

7. Modernise Military Capabilities: Realistic budgeting, self-reliance, joint doctrines, structures, and refined professional military education are crucial for countering future threats. Investment in modernising the armed forces, focusing on advanced technology, C5ISR capabilities, and multi-domain joint force capability is imperative. The existing gap with China must not only be plugged but future multi-domain capabilities generated particularly in the critical oceanic front. Thus, force structuring and modernisation approach must move from threat cum capability to a capability-based approach over long-term planning. Our defence budgeting needs reforms and greater allocation cum efficient utilisation.

8. Deterrence Against Non-State Actors and Terrorism: Strengthening counterterrorism efforts through enhanced intelligence capabilities and international collaboration is vital. In the case of non-state actors, coordinated efforts for intelligence sharing and joint operations are required to address the advanced threat landscape. However, deterring them demands an expansion of the concept and policies of deterrence. These actors operate under different rules, necessitating a thorough understanding of their objectives, leadership, culture and ideologies. Deterrence must address the root cause which often is the toxic ideology rather than just the effects.

9. Cyber Deterrence and Resilience: Enhancing cyber-domain measures to protect critical infrastructure, sensitive information, and financial systems is paramount. Developing a robust cyber offensive and defensive strategy with pre-emptive, proactive, and preventive measures is essential for integrated deterrence.

10. Deterrence in Information Space: The military has made limited progress in addressing IW challenges and implementing its information operations strategy. They have culturally erred in considering information operations as an adjunct rather than as an intrinsic part of operational planning. There is a need for an integrated deterrence strategy with inbuilt offensive and defensive information operations to pursue a competitive advantage, both during war and peace. This would require a cultural shift to effectively integrate information into future deterrence construct.

11. War Stamina and Endurance: The resilience of an indigenous defence industrial ecosystem and robust supply chain emerges as a critical determinant of deterrence. In the context of the era of long protracted wars like the Russia-Ukraine war and the

Israel-Hamas conflict, war stamina and endurance will add to the credibility of deterrence of a nation. India needs to energise its defence ecosystem and asses its war endurance capacities.

12. Missile Warfare: The Iran-Israel missile war has once again brought to the fore the importance of precision warfare by unmanned systems and the need for multi-layered anti-missile and anti-UAV systems. These wars help in controlling the escalation levers while doing tactical damage and strategic influence. Thus they remain an important tool of both deterrence [13]and warfighting. India must invest in both these systems with utmost priority.

Conclusion

In conclusion, the deterrence landscape is complex, dynamic and evolving. Deterrence in the 21st century is not dead but a multidomain integrated complex phenomenon, intricately woven into the fabric of evolving security paradigms that need to be redefined and restructured. As war and peace transform their lexicon, policymakers, as well as scholars, need to deal with the complications brought about by non-state actors, new battlegrounds and escalating threats. India needs to revisit its legacy deterrence[14] construct to make it more potent and relevant to the evolving threat dynamics. This calls for a comprehensive strategy that integrates traditional approaches with modern matrices of deterrence and if deterrence fails then defeating the threat. It must be a combination of deterrence, resilience, and denial to constrain adversaries' hybrid activities across all domains.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

[1] Framing Deterrence in the 21st Century. 18–19 May 2009, RUSI, London. Michael Codner, https://media.defense.gov/2017/Apr/05/2001727306/-1/-1/0/B_0118_DETERRENCE_TWENTYFIRST_CENTURY.PDF

[2] Walter C. Ladwig Iii, Indian Military Modernization and Conventional Deterrence in South Asia, The Journal of Strategic Studies, 2015 Vol. 38, No. 5, 729–772, http://dx.doi.org/10.1080/01402390.2015.1014473

[3] Michael Puttré, Is Deterrence Dead?, Discourse Magazine Jun 2021, https://www.discoursemagazine.com/p/is-deterrence-dead

[4] Michael J. Mazarr, Understanding Deterrence, RAND Corporation, 2018, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf

[5] Echevarria, Antulio J. II, “Deterring War without Threatening War: Rehabilitating the West’s Risk-averse Approach to Deterrence,” Military Strategy Magazine, Volume

[6] James Van de Velde, Cyber Deterrence Is Dead! Long Live “Integrated Deterrence”! NDU Press, JFQ 109, 2nd Quarter 2023, https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-109/Article/Article/3379791/cyber-deterrence-is-dead-long-live-integrated-deterrence/

[7] Mallory, King, New Challenges in Cross-Domain Deterrence. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE259.html.

[8] Lawrence Freedman, The Russo-Ukrainian War and the Durability of Deterrence, IISS DEC 2023, https://www.iiss.org/online-analysis/survival-online/

[9] Avner Golov, Israeli Deterrence in the 21st Century, Memorandum No. 155, Tel Aviv: Institute for National Security Studies, June 2016, https://www.inss.org.il/he/wpcontent/uploads/sites/2/systemfiles/INSSMemo155.03.1.Golov.ENG.pdf

[10] Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd), Indian Military Strategy And Deterrence Paradox, Aug 2021, https://raksha-anirveda.com/indian-military-strategy-and-deterrence-paradox/

[11] Arzan Tarapore, The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance, Carnegie India, Aug. 2020, https://carnegieindia.org/2020/08/10/army-in-indian-military-strategy-rethink-doctrine-or-risk-irrelevance-pub-82426

[12] Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd), Deterrence Paradox Northern Borders, CENJOWS 2022, https://cenjows.in/wp-content/uploads/2022/06/Deterrence-China-by-AB-Shivan-Retd-on-18-Jul-2020.pdf