Analysis of Multi Spectrum Pre-Emptive Threat from China

Brig Arun Sahgal, Phd

Introduction

Chinese discourse on Indian strategic thinking hinges on three broad parameters;

- Conflict with Pakistan can trigger large scale conflict that could engulf China, with inherent risk of nuclear escalation.
- Change in Indian operational mindset. Old passive defence thinking replaced by *'Active defence'* concept, within which '*regional deterrence*' principle is being gradually replaced by *'punishment deterrence'* concept.
- Chinese see this as Indian pro-active approach, as it acquires capacities to conduct *'hi-tech multi domain conventional war backed by credible nuclear deterrence'.*

Conflict Scenarios

Some plausible broad-based scenarios that can trigger pre-emptive actions are:

- "*Teaching India a lesson"* - A rapid defeat of India - i.e. to a point where India suffers visible losses of military capability - diminished stature is seen as consistent with Chinese aim of regional domination.
- *'Territorial gains' most* likely restricted to areas of interest or for bargaining. Nationalistic sentiment post conflict could make territorial swap difficult.
- Chinese rhetoric follows familiar tack of detecting Indian "arrogance"; setting *India – China dispute as a moral transgression*?
- A demonstration that China is able to defend its SLOCs in IOR against Indian interdiction, as the manifestation of Chinese power projection.
- Similarly China would act to protect its partners. Chinese intervention in India-Pakistan conflict or Bay of Bengal/Bangladesh is a possibility we need to plan. Nepal, Bhutan and Myanmar can be used to fan instability.

Factors that will decide when and why China can start conflict with India;

- Perception about both force comparison and geo strategic trends either favourable for strategic coercion alternatively *regional strategic balance emerging in India's favour.*
- Post Dalai Lama insecurity and tensions leading to internal insecurity (Tibet) – initiate border incident?

- *Chinese penchant against surprise might push them to launch a first strike*. In the current strategic discourse. Chinese hysteria about collusive *threat* from India & US could precipitate action?
- *PLA is facing internal challenges plus perception of favourable asymmetry leading to miscalculation. Heightened by Tibetan uprising.*

In all the above scenarios; China's threat to India will be in a *multi-spectrum, pre-emptive environment*, posing complex strategic challenges — spanning conventional, sub-conventional, cognitive, and technological domains simultaneously.

Structured Net Assessment

The Pre-emptive Logic: Why China would act Pre-emptively against India. China's strategic culture favours "active defence" — a doctrine that paradoxically justifies pre-emptive action to deny adversaries ***strategic initiative***. The logic operates against India, across several conditions:

- **Window of opportunity**: China can act before India's military modernization (MRFA, iACS, defence – eco system) matures. Operationalisation of theatre commands will be another factor.
- **Fait accompli Option**: Seize terrain, impose costs, then negotiate from strength — the 2020 Galwan template at a higher scale.
- **Coercive signalling over Kinetics**: Pre-emption need not mean war-initiation; it means shaping India's decision space before India can act thru structured degradation.

The Multi-Spectrum Threat Matrix

Land Domain (LAC plus Salami Slicing)

- Infrastructure asymmetry: China's border road/rail density in Tibet far exceeds India's, enabling rapid mobilization.
- Pre-emptive land grabs: Small, deniable territorial increments below India's escalation threshold — "Gray zone salami slicing" that aggregates into strategic depth loss – difficult to justify politically.
- High-altitude fortress strategy: Permanent village/civilian infrastructure in disputed zones creates facts on the ground, making response politically costly.

- Decapitation of forward positions: In a crisis, China using its tactical mobility and vastly asymmetric capabilities, pre-emptively strikes our forward nodes (Daulat Beg Oldie, Depsang plains) degrading/capturing forward defences before we have had chance to reinforce.

Maritime Domain (IOR Encirclement)

- Maturation of String of Pearls: Gwadar, Hambantota, Chittagong, and potential Maldives/Myanmar basing create a layered presence that could easily transition from commercial to operational in a crisis.
- PLAN power projection: Growing carrier and submarine presence in IOR challenges India's assumed maritime supremacy in its own backyard. American blockade of Strait of Hormuz an example.
- Sea lane interdiction threat: India's energy imports (80%+ seaborne) and trade are vulnerable to pre-emptive maritime coercion — not necessarily sinking ships, but credible threat of interdiction and boarding.
- Submarine pre-positioning: PLAN SSNs/SSBNs pre-deployed in IOR before a crisis would give China immediate escalation options which India will find difficult to counter.

Aerospace and Missile Domain

- PLA Rocket Force targeting: India's strategic assets — Andaman & Nicobar Command, Indian heartland, air and military assets in Eastern and Northern Commands, withing the range of DF-series and CJ-series missiles deployed in Tibet and SW China.
- Anti-satellite (ASAT) pre-emption: India's ISR, navigation (NavIC), and communication satellites are high-value targets. China demonstrated ASAT capability in 2007; pre-emptive blinding of India's space-based C4ISR can be a credible opening move.
- Air superiority pre-emption: J-20s and H-6K bombers operating from Tibetan plateau airfields create standoff strike options that challenge IAF's ability to establish air superiority in a compressed timeline

Cyber and Electronic Warfare

- Critical infrastructure targeting: 2020-21 attacks on Mumbai power grid (attributed to Chinese actors) signal capability and intent — a

pre-emptive physical cyber campaign could degrade India's national critical infrastructure such as communications and mobilization before kinetic actions begin.
- EW spectrum dominance: PLA's EW capability at altitude — including GPS jamming and radar suppression — would degrade India's precision-strike and navigation advantage in a high-altitude conflict.
- Financial/economic cyber pre-emption: India's banking, payment infrastructure, and logistics networks are exposed. A pre-war cyber campaign could induce strategic paralysis without a single bullet being fired.

Cognitive and Information Domain

- Narrative pre-emption: China invests in shaping Indian elite and public perception before a crisis — framing Indian defensive moves as "provocations," dictated by US/QUAD partners. This could complicate India's escalation decisions.
- Political warfare via neighbours: Using Pakistan, Bangladesh, Nepal, and Sri Lanka as instruments of pressure to fragment India's strategic attention — forcing a two-front cognitive load.
- Social media information operations: Targeting Indian domestic political cohesion during a crisis to delay decision-making and create hesitation in political leadership.

Economic Coercion

- Supply chain leverage: India's pharmaceutical, electronics, and solar energy sectors retain critical dependencies on Chinese inputs — potential pre-emptive export controls would impose immediate economic pain. Trade deficit close to $116 billion.
- Investment and debt leverage through neighbours (Pakistan, Sri Lanka, Nepal) creates a coercive economic perimeter around India

The Two-Front Compounding Threat

The most dangerous pre-emptive scenario is orchestrated China-Pakistan action, where:

- China creates a crisis on the LAC, forcing Indian operational attention and deployment, while Pakistan exploits the window for

action in J&K or Punjab through heightened insurgency and pre-emptive force deployment.
- India's strategic reserves and air power are forced to split, creating decision dilemma in terms of impairing response options on both fronts. China need not "win" — it only needs to ensure India gets militarily bogged down against Pakistan. While Pakistan plays a complicit actor.

These are the kind of plausible scenarios, which India’s theatre command structure will need to wargame to assess the nature of capabilities that are required to be developed in multiple domains.

India's Structural Vulnerabilities

Domain Vulnerability

- Intelligence: Limited persistent ISR over Tibet; HUMINT gaps in PLA intent assessment.
- Decision cycle: Civil-military integration slower than PLA's integrated joint operations. We have severe structural issues, which hopefully Theatre Command structure will address.
- Logistics: Forward supply chains still road-dependent; vulnerable to pre-emptive interdiction.
- Space: Limited redundancy in satellite constellation; ASAT defence nascent.
- Cognitive: Political threshold for pre-emptive action remains high; China exploits this vulnerability.
- Partnership Depth: Quad is not a treaty alliance; In environment of fractured ties with US, response to a Himalayan conflict is not guaranteed.

Hedging and Response Posture

India is attempting to close these gaps through organizational reforms and capability enhancement:

- Integrated Theatre Commands (though delayed) once operationalised and integrated will enable faster cross-domain response.
- iSPY constellation and RISAT expansion for persistent border ISR. This is strategic necessity which must become operational by 2028-29.

- AGNI-V/VI and Agni Prime modernization for credible nuclear deterrence against China. India needs to fast track production and deployment of strategic missile force to cover Northern, Western and Maritime theatres.
- IOR dominance investment — P-8Is, INS Vikrant carrier group, expanded Andaman & Nicobar posture. Greater Nicobar as a strategic projection out post is a necessity. India must resolve gaps in under water surveillance, long range anti-ship missile systems, mines and mine warfare etc.
- Strategic Partnerships: Quad and bilateral intelligence sharing (BECA, LEMOA with U.S.) to compensate for ISR gaps.
- Border infrastructure catch-up — BRO's accelerated road/tunnel construction to reduce mobilization asymmetry

Strategic Assessment

China's multi-spectrum pre-emptive threat is designed to constrain Indian threshold response. Not aimed to destroy India militarily, but to make the costs of resistance prohibitive and the benefits of accommodation attractive.

The danger is not a bolt-from-the-blue scenario, but a slow-motion pre-emption across Gray zones that aggregates into strategic disadvantage before India recognizes it as a major conflict.

India's central challenge is developing a credible deterrence posture — the capacity to impose unacceptable costs on China before a *pre-emptive campaign reaches its objectives, across all five domains simultaneously.*

Part II: Cyber - Space Nexus

Strategic Logic: Why Space-Cyber Integration is China's Force Multiplier?

The PLA does not treat cyber and space as separate domains — they are fused into a single "strategic information warfare" envelope under the Strategic Support Force (SSF). The operational concept is well-designed and ruthless: *blind India's sensors*, then act freely in physical domains.

The sequence:

- Space Degradation → ISR Blindness → C2 Disruption (Cyber)

EW Spectrum Dominance → Kinetic Action in Gray/Dark zones. India's entire modern warfighting concept — precision strike, network-centric operations, joint fires — *collapses if the space-cyber layer is degraded first.*

The Space Threat Layer

Anti-Satellite (ASAT) Spectrum: China's ASAT capability has matured well beyond the 2007 Fengyun-1C test. The current threat matrix includes:

- ASAT Type Capability (Direct Ascent KE-ASAT). Threat to Hard kill India's LEO satellites RISAT, Cartosat, NavIC, MEO targets.
- Co-orbital ASAT Manoeuvring "inspector" satellites that can disable/destroy. Deniable, slow-burn — hard to attribute.
- Directed Energy (laser dazzling) Temporarily or permanently blinds optical sensors. Reversible blinding pre-crisis.
- Electronic ASAT Jamming of satellite uplink/downlink. Severs ground-satellite communication.
- Cyber-to-space Hacking ground segment to spoof or disable satellites. No debris, fully deniable

India's specific vulnerabilities:

- NavIC: India's regional navigation system has only 7 satellites. Loss of 2-3 renders the constellation degraded for precision-guided munitions, UAV navigation, and troop coordination. Presently only three satellites are operational.
- RISAT-2BR series: India's primary synthetic aperture radar (SAR) ISR constellation — pre-emptive blinding here means India cannot track PLA force movements in Tibet during cloud cover or night.
- GSAT communication satellites: Military communication links routed through GSAT are vulnerable to jamming and cyber intrusion at the ground segment level.
- Limited redundancy: India has no significant on-orbit spare capacity — lost satellites cannot be replaced in conflict timelines

China's "Soft Kill" Preference: China's preferred opening is likely to be not kinetic ASAT (which creates debris and clear attribution) but reversible soft-kills to include;

- Laser dazzling of optical satellites during critical ISR windows.
- Uplink jamming during crisis to deny real-time imagery.
- Ground station cyber intrusion to corrupt tasking commands.

- GPS/NavIC signal spoofing to feed false navigation data to Indian precision systems

Aim creates strategic ambiguity — India's systems appear degraded, but the cause is unclear, impairing escalatory responses.

The Cyber Threat Layer

Targeting Architecture: China's cyber operations against India likely to follow a three-tier pre-emptive architecture:
Tier 1 — Strategic Paralysis Targets (pre-crisis, long lead).

- Power grid SCADA systems (Mumbai 2020 was a proof-of-concept), Railway network control systems (critical for military mobilization — India moves 70%+ of war materiel by rail).
- Financial clearing infrastructure (RTGS/NEFT disruption during mobilization = logistics payment failure).
- Telecom backbone (disrupt civilian-military communication integration)

Tier 2 — Military C2 Targets (crisis onset)

- Integrated Air Command and Control System (IACCS) — IAF's air defence network.
- Army's Tactical Command, Control, Communication and Intelligence System (Tac C3I).
- Navy's Information Management and Decision Support System (IMDS).
- Border management CCTV/sensor fusion networks on LAC

Tier 3 — Cognitive/Narrative Operations (concurrent)

- Deepfake political leader statements to induce confusion, exploiting social media.
- Fake military orders through compromised channels.
- Social media panic induction in border states.
- Targeting Indian PMO/NSC communication metadata

2. The Pre-Positioned Malware Problem

- The most dangerous aspect is not active intrusion but dormant pre-positioning. Chinese APT groups (APT41, APT10, Stone Panda) have demonstrated years-long persistent access to Indian networks.
- Above implies: Attack code is already inside critical Indian systems Activation requires only a command signal — no infiltration lag time India may not know the scope of pre-positioned access until it's activated.

- Detection and remediation during active conflict is practically impossible

3. Supply Chain Vulnerability
India's dependence on Chinese hardware creates a structural cyber threat:

- Chinese-origin networking equipment, server components, and semiconductors in Indian military-adjacent infrastructure potentially contain hardware backdoors.
- Solar inverters (Chinese-dominated market) with grid connectivity are potential remote-access vectors
- 5G transition vulnerabilities — even where Huawei/ZTE are excluded, component-level infiltration is possible

Crisis Scenario: the Integrated Space-Cyber Kill Chain

The operational scenario at crisis onset:

T-72 hrs: Dormant malware activated in Indian grid/rail SCADA Laser dazzling of RISAT passes over Tibet. NavIC signal spoofing begins in eastern/western sector.

T-48 hrs: IACCS nodes hit with DDoS plus intrusion (air defence degraded). Ground stations for military GSAT jammed. Pakistan-linked hackers (plausibly deniable) hit critical systems in Western Theatre.

T-24 hrs: PLA EW assets activated on LAC — spectrum blackout of Indian forward sensor networks feeding corrupted data. Social media ops peak — false withdrawal orders circulated.

T-0: PLA ground action under ISR/C2 blackout. PLAN submarines surface in pre-positioned IOR locations. PAF activities in J&K under Chinese EW umbrella. *India is effectively fighting blind — its entire intelligence-to-decision cycle is broken before a single kinetic exchange occurs*.

Two-Front Scenario

Design Parameters
Scenario setting: 2027-2029 (near-term, within current force structures)
Trigger: Sustained Indian infrastructure push in Arunachal Pradesh and Ladakh, perceived by Beijing as foreclosing fait accompli options.

Political environment constrained in the backdrop of China – Pakistan and Iran nexus.

Phase 1: Shaping (Six months plus)

China's actions:

- Accelerates "village diplomacy" — new dual-use settlements in Arunachal buffer zones and aggressive actions on the borders.
- PLAN conducts extended IOR "freedom of navigation" exercises, pre-positioning SSKs near Andaman chain (Closer to Myanmar coast).
- Economic pressure: restricts API and other key critical mineral exports (creates domestic crisis narrative).
- Diplomatic: escalates border rhetoric, show of force actions. Recalls ambassador for "consultations".
- Cyber: pre-positioned malware activated in dormant mode — reconnaissance, not attack.

Pakistan's actions:

- Escalates ceasefire violations on LoC and activate ISI sleeper networks in J&K for low-level targeted violence.
- Diplomatic: raises Kashmir at UNSC with Chinese backing, US also lends silent hand.
- PAF conducts exercises near Indian border — ambiguous signals
- Increased drone activity along the LOC and Punjab borders.

India's challenge: Both actions appear independent. Intelligence fusion insufficient to confirm coordination. Political leadership faces domestic pressure on both fronts simultaneously. Political debate on which is the key challenge? Whether to reinforce North or West.

Phase 1: Crisis Ignition (Week 1-2)
Triggering event: Following excessive Indian military activity at DBO and exercises in ALP, WTC orders PLA brigade-level incursion into Depsang Plains. Occupies Indian patrolling points PP10-PP13 with pre-constructed modular fortifications. Simultaneously, "militants" attack BSF convoy in Uri sector with over two dozen casualties.

Cyber-space activation:

- RISAT-2B dazzled during critical overpass — India loses 18-hour ISR window over Tibet. Tata/BSNL backbone routing anomalies begin — military communication latency spikes.

- Fake social media posts: "IAF jet shot down over LAC" — viral within 2 hours, denied 6 hours later.

India's decision dilemma at Week 1: Clearly twin threats are emerging. Critical decision points

- Mobilise Mountain Strike Corps Ladakh/ ALP. To cater for Pakistan front, mobilise, strike reserves in south western and western theatre.
- Keep reserves central or delay action, PLA encroachment of Depsang becomes permanent.
- Escalate to air strikes on PLA positions, risks Chinese strategic retaliation, leads to conflict escalation and attendant consequences.
- Seek diplomatic off-ramp, signals weakness, encourages further salami slicing

The trap is set. India cannot respond decisively on either front without creating vulnerability in the other.

Phase 2: Escalation Ladder (Week 3-6)

Northern Front (China):

- PLA reinforces Depsang with additional mechanized forces — builds helipads and logistics nodes. Extensive mobilisation by PLA ground forces.
- Tibet Military District activates DF-17 hypersonic missile batteries — not launched but positioned visibly (coercive signalling).
- PLAN carrier group enters Bay of Bengal — "transit passage" claim
  China formally announces "defensive posture" — places blame on Indian "provocations"

Western Front (Pakistan):

- Following Indian distraction northward, Pakistan launches "Operation Swift Retort 2" — brigade-level incursion across LoC in Poonch-Rajouri sector.
- PAF executes precision strikes on three IAF forward bases (Adampur/Pathankot/Jammu) — limited but devastating.
- Pakistani Army claims, "response to Indian ceasefire violation" and unwarranted attacks on Terrorist and critical infrastructure — plausible deniability maintained

Indian Air Force dilemma:

- Two-front air war requires splitting air resources over two fronts. IACCS partially degraded by cyber intrusion — air defence coordination impaired.
- IAF strikes Pakistan? Risks Chinese escalation. Strikes China? Risks Pakistani nuclear signalling.
- Maritime and Andaman & Nicobar Command on high alert but cannot be drawn down without ceding space in IOR.

Cyber-space Phase 2:

- Mumbai and Delhi power grids experience "unexplained outages" — civilian panic.
- Indian Railways CTC system hacked — 47 troop trains delayed or rerouted
- NavIC spoofing confirmed in eastern sector — Brahmos targeting data corrupted.
- India's ASAT response option: one test-demonstrated capability, but using it creates debris field over own satellites

Phase 3: Culmination and Strategic Coercion (week 7-10)

China's endgame:

- Depsang fortification complete — new status quo on ground. Offers ceasefire: "India must acknowledge current positions as basis for dialogue".
- PLAN carrier group withdraws from Bay of Bengal — de-escalatory gesture to justify Indian stand-down.
- Frames narrative: India was the aggressor, China exercised "restraint"

Pakistan's endgame:

- Poonch-Rajouri incursion creates new LoC "adjustment", 2-3 km depth.
- Demands UN-mediated ceasefire — China supports it at UNSC.
- Nuclear signalling has frozen Indian conventional response options ISI claims all militant activity was "indigenous Kashmiri resistance"

India's position:

- Territory lost on two fronts without a single declared war. Domestic political crisis — opposition demands accountability.

- Economy hit by cyber disruptions, investor confidence drops.
- U.S. offers "deep concern" statements while advising de-escalation.
- Nuclear deterrent intact but strategically irrelevant at sub-threshold conflict level.

Wargame Lessons: India's critical decision nodes

Decision Nodes

- Phase 1 Depsang: Diplomatic protest. Immediate air-land counter. Rapid heliborne insertion, rapid build-up, plus QPQ operations. international media exposure before fortification completes.
- Phase 1 cyber: Offensive cyber retaliation. Pre-designated retaliatory packages activated automatically as per doctrine.
- Phase 2 Two-Front: Split forces. Prioritise one front. Strategic offensive on Pakistan (faster resolution) while holding on to LAC plus limited QPQ.
- Phase 3 Endgame. Accept ceasefire. Continue resistance or conditional ceasefire — link Depsang to delimitation and demarcation plus economic leverage on China

Red Lines and Escalation control

China’s Redlines

- Indian strikes on Tibet Military District airbases and strategic targets in depth is equivalent to potential nuclear signalling.
- India-U.S. joint ISR operations/ deployment of US Navy assets in IOR and South China Sea, is horizontal escalation of threat.
- Indian naval blockade of Malacca deemed as existential economic threat to China.

India's red lines:

- Pakistani tactical nuclear deployments/use will activate India’s massive retaliation doctrine.
- Chinese naval blockade of Indian ports or interference in SLOC’s particularly in Arabian Sea with Pakistan will result in full spectrum response.
- Cyber-attacks on nuclear command and control is equivalent to crossing existential threshold.

- **The stability paradox**: Both sides have incentives to stay below each other's red lines, which means the two-front Gray zone campaign can persist indefinitely — which is precisely China's preference. Protracted ambiguity favours the aggressor with greater strategic patience.

Strategic Conclusions: Three core findings:

1. The Space-Cyber layer is India's Achilles heel — not the LAC itself. India can fight a conventional border war. It cannot fight one blind, deaf, and with logistics in chaos. *Hardening the space-cyber envelope is more urgent than any additional mountain division*.

2. The two-front scenario is designed to be won below the nuclear threshold — China and Pakistan do not need to defeat India militarily. They need to impose costs high enough that India accepts territorial and political concessions. The wargame ends with India holding nuclear cards it cannot play.

3. India's asymmetric response option lies in the maritime domain — China's Malacca dependency and Pakistan's Gwadar investment are both vulnerable to Indian naval pressure. A credible IOR interdiction threat may be India's most effective deterrent against the two-front trap, as it threatens China's energy security directly.