POLICY BRIEF

From Mountains to Microchips: Technology and India-China Deterrence Stability

Author

Deependra Singh Hooda

Volume VIII, Issue 17

May 23, 2023
ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India’s oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia’s major powers.

Since 2016, in keeping with India’s increasing global profile, DPG has expanded its focus areas to include India’s regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India’s ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India’s national power and purpose, the security and prosperity of the people of India and India’s contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

Author

Lt. Gen. Deependra Singh Hooda (Retd.), PVSM, UYSM, AVSM, VSM & Bar, Senior Fellow for Military Strategy, Delhi Policy Group

The views expressed in this publication are those of the author and should not be attributed to the Delhi Policy Group as an Institution.

Cover Photographs:

Defence Minister Rajnath Singh launched 75 Artificial Intelligence products during the first ‘AI in Defence’ symposium in New Delhi on July 11, 2022. Source: Twitter (@rajnathsingh)

A new BeiDou navigation satellite carried by a Long March-3B carrier rocket is launched from the Xichang Satellite Launch Center in southwest China’s Sichuan Province May 17, 2023. Source: Central Military Commission (China).

© 2023 by the Delhi Policy Group

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003
www.delhipolicygroup.org
From Mountains to Microchips:
Technology and India-China Deterrence Stability
by
Deependra Singh Hooda

Contents

INTRODUCTION .......................................................................................................................... 1
THE IMPACT OF TECHNOLOGY ON DETERRENCE ................................................................. 2
  STRENGTHENING DETERRENCE ......................................................................................... 2
  WEAKENING DETERRENCE ................................................................................................. 4
MILITARY TECHNOLOGY ADOPTION IN CHINA AND INDIA .............................................. 6
  CHINA .................................................................................................................................. 6
  INDIA ................................................................................................................................. 8
IMPACT ON INDIA-CHINA DETERRENCE STABILITY ..................................................... 10
CONCLUSION ......................................................................................................................... 12
FROM MOUNTAINS TO MICROCHIPS: TECHNOLOGY AND INDIA-CHINA DETERRENCE STABILITY
by
Deependra Singh Hooda

INTRODUCTION

In the contemporary era, technology has become omnipresent, driving transformative changes in all aspects of human life. The rapid proliferation of technological innovations has left an indelible mark on modern society, from revolutionising communication and fostering globalisation to reshaping industries and redefining social interactions. Alongside these profound changes, the role of technology in international security and war-fighting has garnered significant attention from scholars, policymakers, and military strategists.

The integration of cutting-edge technologies has altered the landscape of global security and the character of warfare, introducing new challenges and opportunities in the strategic calculus of nations. To avoid being left behind, countries are racing to weaponise emerging technologies such as artificial intelligence (AI), autonomous systems, and cyber capabilities.

Among these developments, the influence of technology on deterrence capability stands out as a particularly compelling area of inquiry, with far-reaching implications for global stability and geopolitical dynamics. This brief delves into the interplay between technology and deterrence, exploring the various ways emerging technologies can both enhance and undermine the traditional paradigms of deterrence theory. As nations grapple with integrating advanced technologies into their military arsenals, the delicate balance of power and the strategic mechanisms that have sustained global stability are increasingly being called into question.

An enquiry into the multifaceted relationship between technology and deterrence is also essential from the Indian security perspective, because deterrence has been an important pillar of India’s national security strategy. The first national military objective in the “Joint Doctrine: Indian Armed Forces” is: “Prevent war through strategic and conventional deterrence across
the full spectrum of military conflict, to ensure the defence of India, our National Interests and sovereignty."¹

Deterrence is very context-specific, is between two adversaries, and is primarily an effort to shape the thinking of a potential aggressor.² Therefore, apart from looking at the general aspects of the impact of technology on deterrence, this brief will also examine the current state of technology adoption in the Indian and Chinese militaries and how this could influence deterrence stability between the two countries.

**THE IMPACT OF TECHNOLOGY ON DETERRENCE**

A RAND study titled ‘Disrupting Deterrence: Examining the Effects of Technologies on Strategic Deterrence in the 21st Century,’ has noted that “collections of emerging technologies—especially in the realms of information aggression and manipulation, automation, hypersonic systems, and unmanned systems—hold dramatic implications for both the effectiveness and stability of deterrence.”³

However, these dramatic implications could be both positive and negative, as emerging technologies have the potential to both strengthen and weaken deterrence. This aspect is explored below.

**STRENGTHENING DETERRENCE**

**Augmented Deterrence Capacities.**

- The advent of emerging military technologies has the potential to enhance deterrence capabilities markedly. Consider, for example, hypersonic weapons. These systems, capable of exceeding Mach 5, can elude most missile defence systems, thereby elevating the potential cost of aggression for adversarial states. Moreover, the speed and precision offered by these weapons equip states with a strategic advantage, strengthening deterrence by framing aggression as a venture fraught with high risk.

AI and autonomous systems further augment deterrence by enhancing decision-making processes, shortening response times, and refining targeting precision. AI-driven surveillance and reconnaissance systems can proficiently detect and track adversarial movements, bestowing military commanders with real-time situational awareness. This heightened awareness and response capability sends a potent signal of a state’s readiness to swiftly and effectively counter aggression, thereby deterring potential adversaries.

Emergence of Non-Kinetic Deterrence

Non-kinetic deterrence signifies a noteworthy departure from conventional forms of deterrence, employing non-physical means to dissuade adversaries from hostile activities. Cyber capabilities present a potent tool for non-kinetic deterrence. States can showcase their ability to infiltrate adversary networks and disrupt critical infrastructure. For instance, the United States’ alleged infiltration of the Russian power grid is a salient example of this form of deterrence, functioning as a cautionary demonstration against further cyber hostility.  

Furthermore, information operations that leverage information and communication technologies can disrupt, corrupt, or manipulate the decision-making processes of adversaries. This might involve disseminating disinformation to create discord and confusion, as exhibited in the alleged Russian interference in the 2016 U.S. presidential election. States can deter adversaries from hostile actions by showcasing their capacity to disrupt the information environment.

Nuclear Reliance: A Shifting Paradigm. The progression and deployment of advanced conventional weapons, such as hypersonic missiles and autonomous systems, could reduce dependence on nuclear deterrence. As these emerging technologies mature, they may present states with a credible alternative to nuclear weaponry. This would enable states to uphold effective deterrence postures without resorting to nuclear arms, potentially reducing the global nuclear arsenals and the associated risks of nuclear conflict.

---

Asymmetric Deterrence: Levelling the Playing Field.

- Asymmetric deterrence, defined as the use of unconventional methods or technologies by a weaker power to deter a stronger adversary, gains new dimensions with emerging technologies. For example, cyber operations can provide a means for smaller states or non-state actors to deter more powerful adversaries, as these operations do not require vast resources or advanced industrial capabilities. Furthermore, AI technologies can enhance information warfare capabilities, serving as an asymmetric deterrent.

- Unmanned systems, such as drones, can also contribute to asymmetric deterrence. These systems are often more affordable and accessible than conventional military platforms, enabling smaller states or non-state actors to field capable forces that can deter aggression. This underscores the transformative role of emerging military technologies in the dynamics of contemporary deterrence.

WEAKENING DETERRENCE

Escalation and Instability. The advent of emerging military technologies, despite their strategic promise, also imbues the geopolitical landscape with risks of rapid escalation and instability. Hypersonic weapons, equipped with unparalleled velocities and evasion capabilities against contemporary defence systems, possess the potential to drastically contract the decision-making timespan during crises. This could trigger impulsive decisions, augmenting the probability of miscalculations or even precipitating responses to falsely perceived threats. Simultaneously, the incorporation of autonomous systems and AI into military operations could lead to unpredictable outcomes. With the threat of human control being overridden, unintended escalations could occur, particularly in the absence of stringent fail-safe mechanisms and control protocols.

Cyber Vulnerabilities and Threats. The increasing reliance on cyber capabilities and digital technologies in military operations exposes new layers of vulnerabilities. The advent of advanced cyber-attacks could incapacitate essential military infrastructures, compromise command and control networks, or manipulate AI-driven operations. These vulnerabilities pose a formidable threat to the efficacy and reliability of deterrence by fostering uncertainty about a state's capacity to counter aggression. Thus, while cyber capabilities expand the horizons of deterrence and warfare, they simultaneously expose states to unique forms of disruption and attack.
Arms Race Dynamics. The emergence of novel military technologies could spur competitive dynamics among nations, potentially fuelling a new type of arms race. The progression and deployment of new technologies could catalyse nations into a spiralling contest for technological dominance. This escalating competition could exacerbate military tensions, prompting states to invest heavily in cutting-edge technologies to prevent strategic inferiority, potentially destabilising the global security architecture.

Erosion of Norms and Legal Frameworks. The integration of emerging technologies into military systems presents formidable challenges to established norms and legal frameworks governing warfare. The deployment of autonomous weapons systems, for instance, raises critical questions about accountability and compliance with international humanitarian law. Similarly, the utilisation of cyber capabilities in deterrence and warfare blurs the traditional distinction between peace and war, complicating the application of established norms and laws. This ambiguity could result in the potential misuse of technologies and complicate conflict resolution and international relations.

Inequality and Asymmetric Threats. The dissemination of emerging military technologies threatens to exacerbate global disparities and spawn novel asymmetric threats. Technologically advanced states stand to amass significant strategic advantages, potentially disrupting the equilibrium of deterrence and fostering power asymmetries. Conversely, non-state actors, insurgents, or rogue states may exploit these technologies to pose asymmetric threats, thereby complicating traditional deterrence paradigms. Moreover, the availability of commercial off-the-shelf technologies, such as drones, could be weaponised, contributing to a progressively complex and challenging security milieu.

In sum, while emerging military technologies offer substantial opportunities to augment deterrence, they concurrently introduce considerable challenges and risks to deterrence. Which way the balance will swing will depend on whether adopting new technologies gives a significant advantage in the balance of military power between two adversaries.

Several factors, like capabilities, perceptions and motivations of the potential aggressor, miscommunication, risk tolerance, etc., influence the success or failure of deterrence. Among these, military power plays a significant role. According to John J. Mearsheimer, deterrence occurs “when a potential aggressor realises that his military forces are not capable of achieving their
battlefield objectives.” Henry Kissinger echoes the same sentiment: “Deterrence depends on a combination of power, the will to use it, and the assessment of these by the potential aggressor.” Without adequate military power, deterrence will inevitably weaken.

It is important to point out that technology adoption is not merely the possession of technology. As Christopher Chyba points out, “The ability of a state to develop and deploy a technology with sufficient salience to alter strategic stability depends on factors that go beyond the readiness and scope of the technology. These include financial and organisational requirements as well as the extent to which adopting the technology would disrupt existing military practice or the status of relevant organisational elites.” Therefore, appropriate organisational structures and operational concepts must be developed for the optimum utilisation of technologies.

After looking at the general aspects of how technology could impact deterrence, we now turn specifically to China and India. The next two sections of the brief explore the adoption of emerging military technologies in China and India and its likely bearing on deterrence stability between the two countries.

**MILITARY TECHNOLOGY ADOPTION IN CHINA AND INDIA**

**CHINA**

China’s 2019 Defence White Paper states that the People’s Liberation Army (PLA) has “made great progress in independent innovation in some strategic, cutting-edge and disruptive technologies, and succeeded in developing strategic hi-tech products such as the Tianhe-2 supercomputer. Focusing on war and fighting wars, China’s armed forces have innovated in military doctrines and delivered outcomes in military strategy, joint operations and informationisation which have provided a theoretical support to defence and military development.”

---

China has been investing heavily in military technology and capabilities to become a global military power. As part of its strategy to develop the PLA into a “world-class military” by 2049, China’s Military-Civil Fusion (MCF) plan has been elevated to a national strategy. MCF seeks to deepen the interaction between China’s civil research, commercial sectors, and the military. The MCF targets key technologies like quantum computing, big data, semiconductors, 5G, advanced nuclear technology, aerospace technology, and AI.9

Supporting the MCF is the “Made in China (MIC) 2025”. The plan aims to transform China into a leading manufacturing power by developing ten high-tech industries. These include information technology, high-end numerically controlled machine tools and robots, aerospace equipment, and new materials, such as polymers.10

China has prioritised research and development (R&D) in the military sector, focusing on hypersonic weapons, stealth technology, unmanned systems, artificial intelligence, and quantum technology. Although exact figures are not known, it is estimated that China spends approximately 20 per cent of its defence budget on R&D.11 That would put its current annual military R&D spending at about $45 billion.

The 2023 Australian Strategic Policy Institute’s (APSI) Critical Technology Tracker notes that in the defence, space, robotics and transportation sectors, China leads the world in four out of six categories - advanced aircraft engines (including hypersonics), drones, swarming and collaborative robots, autonomous systems operation technology, and advanced robotics. China is also the leader in other areas that have defence applications – quantum communications, biotechnology, directed energy technologies, artificial intelligence and data analytics, and protective cybersecurity technologies.12

In 2015, China dramatically restructured the PLA, eliminating China’s seven military regions and converting them into five theatre commands. A new

---

Strategic Support Force (SSF) was raised to integrate capabilities for space, cyber, electronic, and psychological operations. The SSF is at the forefront of acquiring technology and has invested heavily in AI for intelligence; surveillance and reconnaissance; autonomous vehicles; information and electronic warfare; simulation and training; predictive maintenance; and target recognition.13

China’s 2019 Defence White Paper notes that “war is evolving in form towards informationised warfare, and intelligentised warfare is on the horizon.” Several Chinese researchers explain this concept as “integrated warfare waged in land, sea, air, space, electromagnetic, cyber, and cognitive arenas using intelligent weaponry and equipment and their associated operation methods, underpinned by the IoT [internet of things] information system.”14 In this direction, the PLA is exploring next-generation operational concepts for intelligentised warfare, such as attrition warfare by intelligent swarms, cross-domain mobile warfare, AI-based space confrontation, and cognitive control operations.15

INDIA

India also has the potential to exploit new technologies. According to the ASPI Critical Technology Tracker, India is among the top five countries in two of the six categories of the defence, space, robotics and transportation sector. India figures in the top five in nine out of ten categories in AI, computing and communications.

Despite its potential, India’s adoption of new military technologies is relatively slower than China’s. There are two primary reasons for this. The first is inadequate spending on R&D. India spends approximately 0.7% of its GDP on R&D compared to 2.1% in China.16 In 2022, Indian and Chinese R&D

expenditure was $65.2 billion and $551 billion, respectively.\textsuperscript{17} Indian spending on defence R&D is 4% of its defence budget, totalling approximately $3 billion.

The second reason is that India lacks a sufficiently capable defence industry with the capacity to develop and produce highly sophisticated arms. As a result, India was the largest importer of arms in the world in the period 2018-22.\textsuperscript{18} Even where there is expertise within the country, e.g., in the information technology sector, reliance is still on foreign hardware and software.\textsuperscript{19} It is evident that exporting countries rarely part with cutting-edge technology, and these will have to be developed indigenously.

In recent years, the government is giving a push for greater indigenisation under the policy of AtmaNirbhar Bharat (Self-Reliant India). Since 2020, the government has notified 411 items that would be progressively banned for imports between December 2021 and December 2032.\textsuperscript{20} To make India’s ordnance factories more efficient, the Ordnance Factory Board has been corporatised.\textsuperscript{21} In August 2020, Prime Minister Narendra Modi announced 74% foreign direct investment in defence production through the automatic route to “increase production in India, develop new technology..., and maximise expansion of private sector in defence.”

The AtmaNirbhar Bharat is an extremely important initiative, but no short-term results should be expected as it will take time for the defence industry to mature.

In some of the cutting-edge technology areas, India has taken the initial steps. For example, the Indian military has raised a Defence Cyber Agency, a Defence


Space Agency, and a Special Operations Division. The military’s demand was to raise these as command-level organisations, but even the smaller structures will provide integrated capability development that was missing.

To implement the future use of AI in defence applications, the Defence AI Council (DAIC) and a Defence AI Project Agency (DAIPA) were set up in 2019. On July 11, 2022, the Indian Defence Minister, Rajnath Singh, launched 75 newly developed AI Technologies. However, what is still lacking is the integration of data that still resides in service silos.

India has tested a Hypersonic Technology Demonstration Vehicle, but its operationalisation could take another four to five years. In the field of unmanned systems, India has not yet developed an indigenous armed UAV and is still dependent on imports.

**IMPACT ON INDIA-CHINA DETERRENCE STABILITY**

As mentioned earlier, India’s primary national military objective is to prevent war through strategic and conventional deterrence. For India, deterring China from military action has been a function of two factors. The first factor is geography. The Himalayan watershed that runs along a large part of the LAC is a formidable obstacle, and the PLA would find it extremely difficult to launch major operations across it. India’s geography also gives it a dominant position in the Indian Ocean. The PLA Navy has been growing at an unprecedented pace, but to undertake operations in the Indian Ocean, it has to overcome its weaknesses in Maritime Domain Awareness (MDA), tactical air cover, communication infrastructure, and strategic anti-submarine warfare.\(^{22}\)

The second factor has been India’s conventional military strength. The Indian Army has a powerful deployment along the LAC and the Indian Air Force has an advantage of air operations over Tibet, operating from airfields in the plains whereas the PLA Air Force operates from high-altitude airfields. Furthermore, currently the Indian Navy cannot be seriously challenged by the PLA Navy in the Indian Ocean. Therefore, there has been a strong element of ‘deterrence by denial’ premised upon China’s fear of failure in achieving a decisive victory.

Nonetheless, as emerging technologies reshape the contours of warfare, there is a risk that India’s deterrence could weaken. If the technology gap between the two countries results in widening the military capability differential,

---

deterrence stability between India and China could be adversely impacted. Some emerging technologies like hypersonics, unmanned systems, electronic warfare, cognitive warfare, perception manipulation technologies, and quantum technology could help China surmount physical barriers that have traditionally reinforced India’s deterrence posture.

In December 2019, China reportedly deployed a fleet of underwater drones in the Indian Ocean to gather data that could be used for improving the detection capability of Chinese anti-submarine warfare. In 2022, China launched Zhu Hai Yun, a semi-autonomous ‘drone mothership’ capable of carrying multiple autonomous UAVs, boats, and submersibles for reconnaissance and ocean surveillance. It is reportedly provided with an AI operating system enabling it to launch, recover and coordinate up to 50 autonomous platforms. Similar developments in the future could help the PLA Navy overcome some its current weaknesses in the Indian Ocean.

If China feels it has a decisive military edge, it could be tempted to use military force to gain a quick victory or continue with protracted salami-slicing. Overconfidence in one's military capability can lead to deterrence failure and potentially heighten the prospects of conflict. Even if direct military force is not used, China could engage in grey zone warfare and limited incursions along the LAC to keep up the pressure on India. Some of the technologies like cyber and perception manipulation make attribution difficult, and China could use these aggressively against India.

The Chinese mouthpiece Global Times puts out regular commentaries on how “India is not militarily capable” to fight a “powerful China” and the “PLA is bound to make the Indian Army suffer much more severe losses than it did in 1962.” Some of these remarks may be for the domestic audience, but misperceptions about military capability can encourage risk-taking behaviour.

As the PLA increasingly adopts AI and autonomous systems, the use of force is more likely as the human cost of the conflict is reduced. Decision-making by AI systems controlling autonomous machines could lead to a quick escalation

---


of a crisis. The widespread use of misinformation, deep fakes, propaganda, and perception manipulation would make it almost impossible to get a clear idea about the intentions and redlines of the two countries, thereby amplifying the risk of conflict.

If India’s national security is to be strengthened, it must be ensured that the technology gap with China does not become so large that it undermines India’s deterrence strategy. It could be stated that India will always be playing catch-up because it cannot invest as heavily as China in military technology. While this may be true, a targeted approach can be adopted towards the development of specific technologies that can neutralise China’s advantages.

The Indian military must prioritise technologies that strengthen ‘deterrence by denial’ by reducing the effectiveness of China’s military capability and putting doubts in its leadership’s mind about the results of a military conflict with India. For this, there is a need to create appropriate structures and clearly articulate strategies for the adoption of technologies and their role in future war-fighting.

The Indian military could look at combining cyber, space, electronic warfare, and information warfare under a joint command. This would help in integrating a diverse range of technologies for wartime employment. A ‘Futures Directorate’ should be created under the CDS with two verticals: one to look at emerging technologies and plan for their induction into the military, and the second to develop a doctrine for a future war fought with emerging technologies. The effectiveness of technologies is determined to a large extent by the operational concepts for their employment.

The Defence Research & Development Organisation (DRDO) must also be restructured to focus on specific cutting-edge technologies. With 52 labs and a workforce of approximately 25,000, almost half of the DRDO’s budget goes into revenue expenditure. Some of the low-technology research must be outsourced and the DRDO must become a leaner organization with maximum funds utilised for R&D.

**CONCLUSION**

Emerging technologies are not only revolutionising the character of war but could also affect the credibility of deterrence. Technologies have the potential to both strengthen and weaken deterrence stability. Which way the balance

---

swings will depend on whether the adoption of technologies significantly alters the balance of power between two adversaries.

China has invested heavily in advanced military technology and created organisational structures and concepts for intelligentised warfare. India is also looking to incorporate new technologies into the military, but is somewhat hampered by inadequate spending in R&D and the slow pace of indigenisation.

In case China and India's adoption of military technologies widens the already significant power differential in favour of China, India's deterrence strategy could weaken. This could embolden China to rely on military force, either directly or indirectly, to shape the strategic environment. It is, therefore, essential for India to focus on technologies that strengthen 'deterrence by denial,' create appropriate organisational structures, develop operational concepts, and majorly review the functions of the DRDO.

***