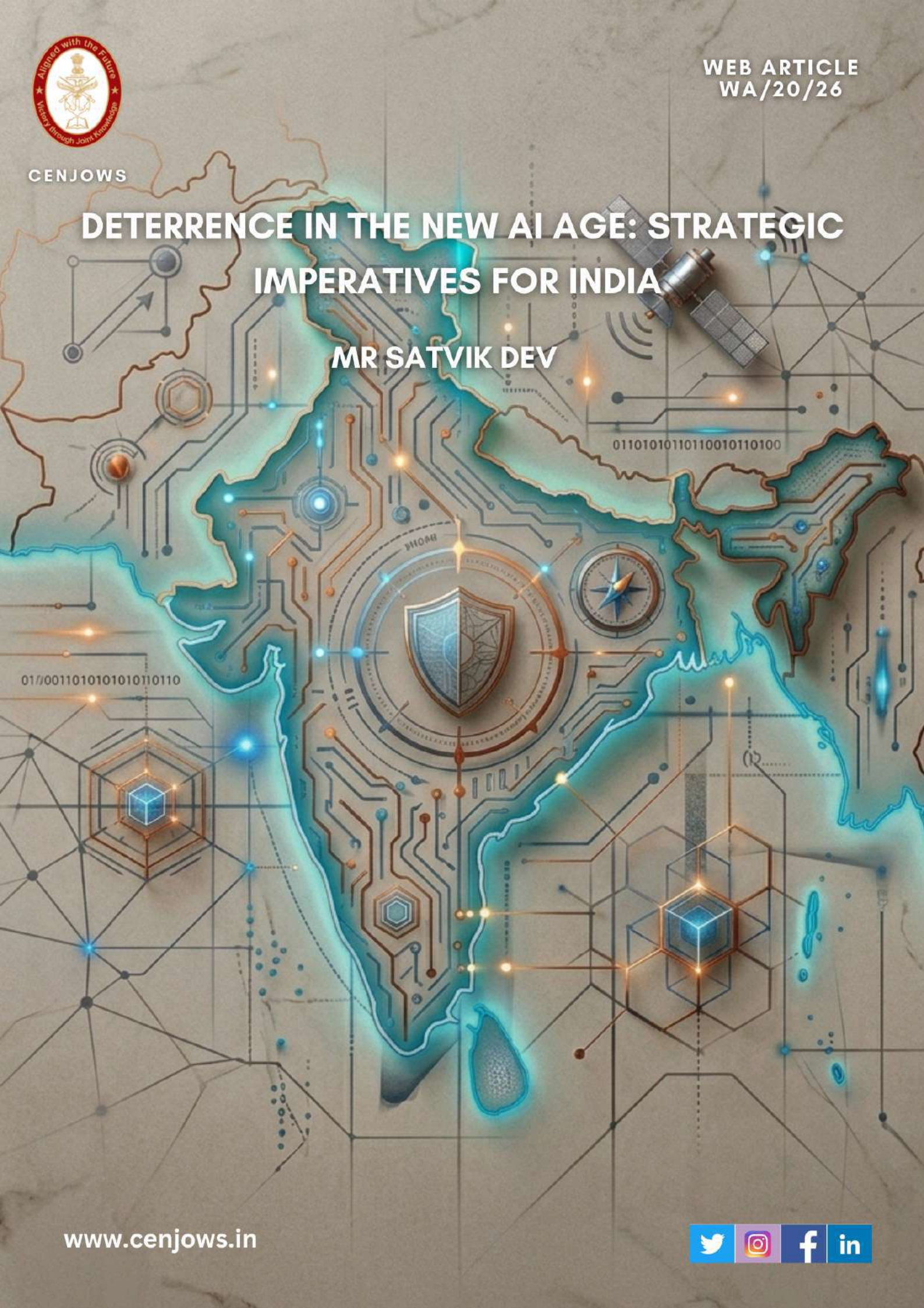
WEB ARTICLE
WA/20/26

CENJOWS

DETERRENCE IN THE NEW AI AGE: STRATEGIC IMPERATIVES FOR INDIA

MR SATVIK DEV



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Deterrence in the New AI Age: Strategic Imperatives for India

Satvik Dev is a research intern at CENJOWS

INTRODUCTION

In September 2022, Elon Musk reportedly directed one of his SpaceX employees to cut off Ukraine's access to Starlink. This satellite-based internet service had become crucial for the Ukrainian military's battlefield connectivity. This decision resulted in a sudden communications blackout for Ukrainian troops who were simultaneously undertaking a counteroffensive operation to reclaim an occupied territory from the Russian forces. According to an official, the immediate consequences were severe as "soldiers panicked, drones surveilling Russian forces went dark, and long-range artillery units, reliant on Starlink to aim their fire, struggled to hit targets."[1] This episode marked one of the most profound illustrations of 'corporate autonomy' whereby a private transnational company exercised its digital infrastructural power to constrain a sovereign state's coercive and operational capabilities in a kinetic conflict theatre.[2]

In this regard, the paper argues that the international order is currently undergoing a structural shift. It stresses how Big Tech actors, equipped with substantial financial resources and technological capital, exercise a renewed agency in shaping outcomes across political environments. This has significant ramifications for traditional security and highlights what potential policy actions can be explored by India to tackle these new sets of challenges that have become apparent.

PRIVATE PROWESS: AI AND SEMICONDUCTORS

The recent decades have witnessed a meteoric rise in private sector R&D investment, coupled with a dense, networked coordination of technology firms that has been simultaneously reinforced by the entrenchment of state power.[3] This innovation-led expansion of certain firms has resulted in a systemic shift from the government's hold over public information/data to a monopoly increasingly being exercised by private sector companies.[4] The scale of this diffusion in control over nodality, from state to corporate domain, is evident from the fact that "in 2023, industry produced 51 notable machine learning models vis-a-vis academia's 15, thereby far outstripping any other institution's contribution to public sector AI."[5] Additionally, as the lines between civil and military technologies tend to blur with rapid innovations across dual-use domains, the centrality of these Big Tech firms like Alphabet, Meta and Microsoft is only likely to expand further. The key agents driving this growth would be entities like OpenAI and Anthropic, which, besides having "their foundation models integrated into everyday chatbots and AI assistants", would also be incorporated into state security and defence architecture.[6] An illustrative example would be the recent deployment of Anthropic's Claude model by the Pentagon. The suite of proprietary large language models, along with other tools, was embedded into Palantir software and was crucial in US military operations undertaken in both Venezuela and Iran.

These private firms' consistent grip over their power largely stems from the competition surrounding the strategic hold of semiconductors in modern-day geopolitics. These advanced microchips, which hold billions of transistors responsible for electrical conductivity, have effectively become a foundational resource without which virtually no piece of modern technology can function.[7]

It is precisely the sway exerted by certain private firms in this sphere that has led scholars to claim this new emerging order as technopolar.[8]

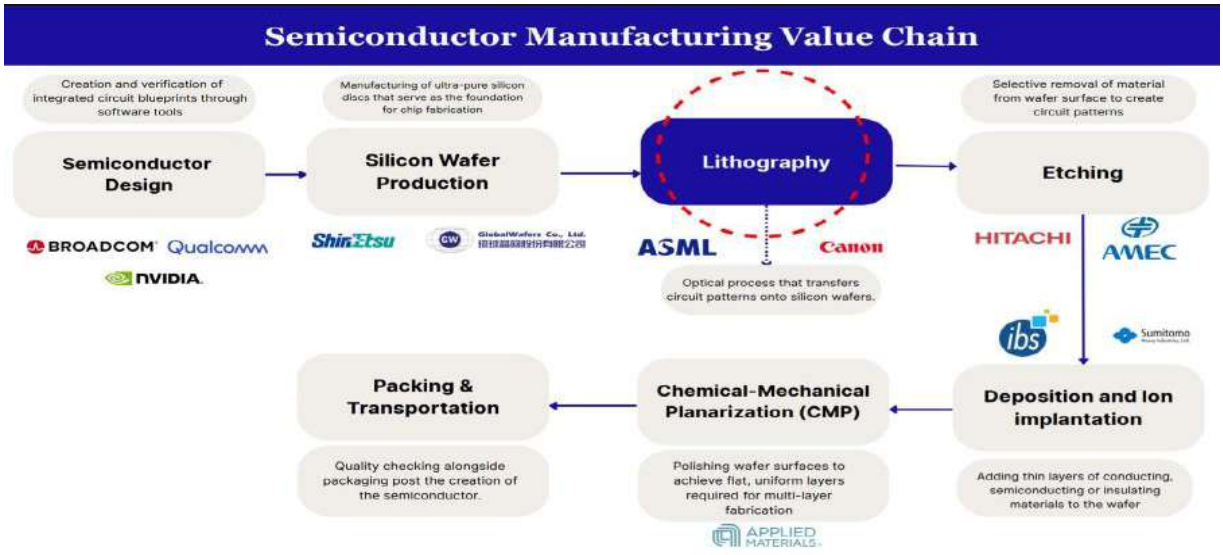


Figure 1 (FOI, Ashoka University)

A majority of the critical stages of the semiconductor ecosystem, from chip licensing and designing to manufacturing and fabrication, are dominated by private firms (as evident from *Figure 1*). While Netherlands-based ASML remains the sole manufacturer of the EUV lithography machines essential for printing circuits onto a silicon wafer, US-based Nvidia and Taiwan-based TSMC exercise global monopoly over designing and manufacturing of high-grade chips, respectively.[9] This has turned the private enterprise into an indispensable stakeholder in international politics.

NEW COLD WAR: INFORMALITY AND CRISIS FOR SMALL STATES

It is important to note that the chief attributes of this new emergent order, by no means, imply a wholesale erosion of state authority. Despite a largely private ownership of these key chokepoints, these firms continue to remain subject to state oversight and geopolitical pressures, especially in dimensions concerning trade and technology transfer. For instance, the US officials under the Trump administration have successfully lobbied the Dutch government since 2019 to ban the export of ASML's advanced EUV machines to China.[10] The underlying idea is that while major powers shall retain a certain threshold of authority, this unprecedented diffusion of power will

inevitably reform the way many global supply chains are governed. This would entail a gradual dissolution of the formal rules-based apparatus, marking a transition to an informal arrangement concerning domains like trade and security, worked out discreetly by states and technological conglomerates.[11]

While such a framework works ideally for states already possessing deep inroads in the semiconductor value chain, it would create huge impediments for other states that may eye themselves as prospective entrants but lack the material capabilities to accomplish wholesale reshoring of these facilities. The task of attracting critical manufacturing companies to one's domestic soil for semiconductor production is extremely challenging, and the prospect of duplicating entire supply chains imposes too high a prohibitive cost beyond the capacity of smaller powers.[12]

This appears to be further amplified with the emerging technological rivalry between the US and China regarding the dominance over full-stack manufacturing chains of semiconductor chips. Amidst the rising economies, China's ambitions of attaining technological self-sufficiency have been evident since the release of its comprehensive national security white paper in 2014. This has placed it at loggerheads with the United States, whose growing paranoia under the Trump administration regarding its dilapidating influence has only exacerbated the issue. This has been captured aptly by journalists Bob Davis and Lingling Wei in their joint work called Superpower Showdown (2020). Building on the history of challenges inherent in the trade negotiations between the two States, the authors contend that increased polarization may lead to a new form of cold-war-like rivalry.[13] It would not only foster apprehension among all existing states but may also compel each to join one bloc over the other.

Such a configuration would only accentuate the uncertainty faced by other rising powers who are already constrained by a limited bandwidth to proceed with caution. Following on previous discussions, these states would not only be required to calibrate their relationships with both great powers, but in a new fashion, would also have to systematically assess and chart out strategic partnerships with powerful technology firms.

While certain states like Japan, South Korea and the Netherlands may retain a sort of veto power owing to their pivotal roles in the semiconductor manufacturing chain, others would largely be subjected to pressures to extend concessions to either side. These pressures, amongst other dimensions, would entail serious ramifications for the security and economies of these states.

ENVISIONING DETERRENCE IN THE TECH DOMAIN

Accordingly, states need a more calibrated approach in navigating this evolving landscape. A key concept which continues to hold prominence in scholarly discourse surrounding this subject is deterrence theory. Traditionally developed with respect to nuclear weapons, the idea of deterrence at its core, refers to "the ex-ante dissuasion of adversaries through the threat of ex-post costs in response to potential adversary actions".[14] The logic is to create a perceived cost within the calculus of the adversary high enough that it gets dissuaded from engaging in any offensive cost against the incumbent actor. This perceived cost on the adversary could take two principal forms. Either it would instil a belief of an imminent failure in terms of achieving the objectives of the offence, i.e., deterrence by denial or a fear of massive retaliatory strike resulting in huge material and immaterial damage for the adversary, i.e., deterrence by punishment.[15] While this has mostly been limited to the military sphere, these changing circumstances have generated a pressing need for state actors to expand deterrence to cover the entire range of options available in navigating such a complex landscape in future.

Consequently, this necessitates huge strategic implications for India as well. Despite being a rising economic powerhouse, India's status is significantly weakened by its limited influence in the semiconductor ecosystem compared to the US or China. While it houses roughly 20% of the world's chip design work talent, it lacks any significant advantage in the manufacturing segment. Policy experts have repeatedly laid emphasis on how a more conscious and streamlined approach is imperative to foster conditions that could enable the emergence of a regional manufacturing hub. Recent investment drives culminating in 9.6 billion dollars under the India Semiconductor

Mission (ISM), along with a network of state-level tax rebates and incentive schemes, signal a positive trend.[16] However, despite these efforts towards attaining the necessary prerequisites, severe structural challenges still persist.

India's domestic industry remains highly vulnerable to supply chain shocks, especially in terms of raw materials like silicon wafers, high-purity gases, speciality chemicals, and ultrapure water, over 90% of which are imported.[17] Furthermore, despite producing a high number of engineers annually, India faces a shortage of skilled workforce required for advanced tasks such as fabrication, packaging and precision equipment maintenance. Besides these issues, a deeper problem lies with India's inefficient research and development (R&D) pipeline. Besides the US and China, which lead the global spending on R&D in the semiconductor industry in absolute terms, almost all other major powers also lie miles ahead of India in terms of R&D spending as a percentage of GDP. States like South Korea and Israel invest roughly 4.9% and 5.6%, respectively, in future-proofing their economies and militaries compared to India's abysmal 0.64%.[18] This dynamic critically impacts the nature of industrial output which emerges. At present, most operational facilities that are coming up in Bengaluru, Gujarat, and Chennai are oriented towards assembly and packaging activities, which are being led by Western technology giants. The limited role of domestic private companies in higher-value segments of the manufacturing chain has restricted India to a largely service provider role on a global scale within the semiconductor ecosystem.[19]

STRATEGIC IMPERATIVES FOR INDIA

Such a position in the long run could seriously restrict India's options in terms of establishing credible deterrence against a formidable adversarial nexus between private tech and a great power. The entire idea of punishment, which has increasingly come to inform India's conventional military doctrine with respect to cross-border terrorism along its western front, rests on the possession of sufficiently advanced capabilities to ensure effective punitive retaliation.[20]

Within the digital sphere, these capabilities would roughly correspond to securing a lion's share in the contribution towards the crucial higher value segments of semiconductor manufacturing, halting which would disrupt the entire cycle. However, since India's role in the AI stack production chain is limited, it gravely lacks the capabilities to do so.

Under these circumstances, the immediate measures regarding technological aspects of national defence and security ought to be denial-based. Since a majority of private investment drives are being spearheaded by foreign firms, a market denial strategy could prove self-detrimental in terms of the sheer losses of jobs within India that can have a cascading effect, leading to further political instability. Hence, the calculus remains restricted to largely two options which could plausibly be pursued.

One approach could be a 'Multi-Homing' manoeuvre, which would entail investing in a multi-vendor defence architecture.[21] India could integrate components sourced from multiple partners, such as US-made GPUs and sensors from Japan, into the Indian RISC-V-based indigenously developed processors, such as SHAKTI, designed by IIT Madras.[22] This flows naturally from India's long-standing strategic autonomy discourse, thereby enabling it to avoid excessive dependency on a single external actor, say the US, by using an indigenous design and boost its bid for digital sovereignty in the long strategic sphere.

A second approach could focus on incorporating Edge AI in Tactical Defence Networks, which would entail reducing military dependence on frontier models like GPT and Claude, which operate on cloud computing infrastructure. Instead, latent entrants like India could focus on incorporating Edge AI mechanisms into their frontline military units. In a battlefield environment akin to one highlighted in the beginning of the article, disruption in lines of communication from command centres located afar can severely compromise the operational capabilities of troops on the ground. In such a case, as Wentz highlights, "processing data at the edge shortens the OODA loop - the cycle of observing, orienting, deciding and acting by turning the raw sensor input into usable insights on the spot".[23]

The idea of drone teaming, whereby several drones fly with “embedded processors running autonomy software directly on the aircraft” and “coordinate routes and strike decisions locally”, precisely captures this.[24] It is already in its implementation phase in the US and Chinese military infrastructures.

This is further plausibly achievable since smaller and more specialized models can run on 28nm or 65nm chips, for which India is not entirely dependent on TSMC production. The key takeaway, therefore, in terms of short-term policy maneuvers is to ensure deterrence in the dynamic technological realm by transitioning and adopting actionables that focus on indigenously driven technology use in key sectors such as the military. This has to be coupled with the objective of building domestic resilience simultaneously for long-term success.

DISCLAIMER

The paper is the author’s individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. 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] Joey Roulette, Cassell Bryan-Low, and Tom Balmforth, “Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory From Russia,” *Reuters*, July 27, 2025, https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/.

[2] Dennis Broeders, Arun Sukumar, Monica Kello, and Lise H. Andersen. 2025. “Digital Corporate Autonomy: Geo-Economics and Corporate Agency in Conflict and Competition.” *Review of International Political Economy* 32 (4): 1189–1213. doi:10.1080/09692290.2025.2468308.

[3] Swati Srivastava and Justin Bullock, “AI, Global Governance, and Digital Sovereignty,” Convergence Analysis, (2024).

[4] Matt Birkinshaw and Sanjay Srivastava, “CONSULTANCY STATE: Government as (a) Service and the Anti-politics of Technological Expertise in Indian Cities,” International Journal of Urban and Regional Research, January 20, 2026, https://doi.org/10.1111/1468-2427.70061.

[5] Kevin Klyman, Aaron Bao, Caroline Meinhardt, Daniel Zhang, Elena Cryst, Russell Wald, and Fei-Fei Li. “Expanding academia’s role in public sector AI.” Issue Brief. HAI Policy & Society, 2024.

[6] Swati Srivastava and Justin Bullock, “AI, Global Governance, and Digital Sovereignty,” Convergence Analysis, (2024).

[7] Chris Miller, “Chip War: The Fight for the World’s Most Critical Technology.” Simon and Schuster, 2022.

[8] Bremmer, Ian. “The Technopolar Moment: How Digital Powers Will Reshape the Global Order.” Foreign Affairs 100, no. 6 (2021): 112–28. https://www.jstor.org/stable/27121446.

[9] Miller, “Chip War: The Fight for the World’s Most Critical Technology.” 2022.

[10] John Krige, "Debate: Building a U.S. Regulatory Empire in the Chip War with China." Technology and Culture 65, no. 4 (2024): 1081-1108. https://dx.doi.org/10.1353/tech.2024.a940462.

[11] Sukumar et al., “The Pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy”, Contemporary Security Policy 45, no. 1, 2024.

[12] Sujai Shivakumar and Shruti Sharma, “Semiconductor Clusters in the Making: India’s Push for Global Competitiveness,” *CSIS*, February 13, 2026, https://www.csis.org/analysis/semiconductor-clusters-making-indias-push-global-competitiveness.

[13] Bob Davis and Lingling Wei, “Superpower Showdown: How the Battle Between Trump and Xi Threatens a New Cold War”, Harperbusiness, 2020.

[14] Aaron F. Brantly, “The cyber deterrence problem,” NATO CCD COE, May 1, 2018, 31–54, https://doi.org/10.23919/cycon.2018.8405009.

[15] Lawrence Freedman, “Introduction—The Evolution of Deterrence Strategy and Research.” In: Osinga, F., Sweijs, T. (eds) NL ARMS Netherlands Annual Review of Military Studies 2020. NL ARMS. T.M.C. Asser Press, The Hague. 2021. https://doi.org/10.1007/978-94-6265-419-8_1

[16] Vaibhav Chhimpa, “Strategic Redundancy in Semiconductor Supply Chains: How US-India Cooperation Transforms Global Chip Resilience’, SAIS review of International Affairs, (2025).

[17] ANI, “India’s Semiconductor Industry Faces Supply Chain and Limited Talent Challenges: Jefferies Report,” *The Economic Times*, 2025.https://economictimes.indiatimes.com/tech/technology/indias-semiconductor-industry-faces-supply-chain-and-limited-talent-challenges-jefferies-report/articleshow/119453491.cms?from=mdr.

[18] Samreen Wani, “India’s Expenditure on R&D Just 0.6 Percent of GDP: Economic Survey,” January 29, 2026, https://www.forbesindia.com/article/budget-2026/indias-expenditure-on-rd-just-0-6-percent-of-gdp-economic-survey/2990842/1?hl=en-GB.

[19] Karan Dhar, “India’s R&Amp;D Spend at 0.6% of GDP Due to Low Contribution From Private Sector: Economic Survey,” Business Today, January 29, 2026, https://www.businesstoday.in/economic-survey/story/indias-rd-spend-at-06-of-gdp-due-to-low-contribution-from-private-sector-economic-survey-513453-2026-01-29?hl=en-GB.

[20] Tami Davis Biddle, “Coercion Theory: A Basic Introduction for Practitioners (Spring 2020),” Texas Digital Library (University of Texas), January 1, 2020, https://doi.org/10.26153/tsw/8864.

[21] Lt Gen Karanbir Singh Brar, “Manoeuvring Technology: Redefining Military Strategy in the Era of MDOs,” orfonline.org, September 30, 2025, https://www.orfonline.org/expert-speak/manoeuvring-technology-redefining-military-strategy-in-the-era-of-mdos#:~:text=Traditionally%2C%20manoeuvre%20meant%20the%20deliberate,with%20far%20greater%20situational%20awareness.

[22] Press Release - IIT Madras, *“IIT Madras & ISRO Jointly Developed and Successfully Booted an Atmanirbhar Aerospace Quality SHAKTI-based Semiconductor Chip”* , February, 2025. https://www.iitm.ac.in/happenings/press-releases-and-coverages/iit-madras-isro-jointly-developed-and-successfully-booted

[23] Jacob Wentz “Harnessing Edge AI to Strengthen National Security | CSIS,” 2025, https://www.csis.org/blogs/strategic-technologies-blog/harnessing-edge-ai-strengthen-national-security.

[24] Ibid, 2025.