SRGF
STRATEGY - RESEARCH - GROWTH

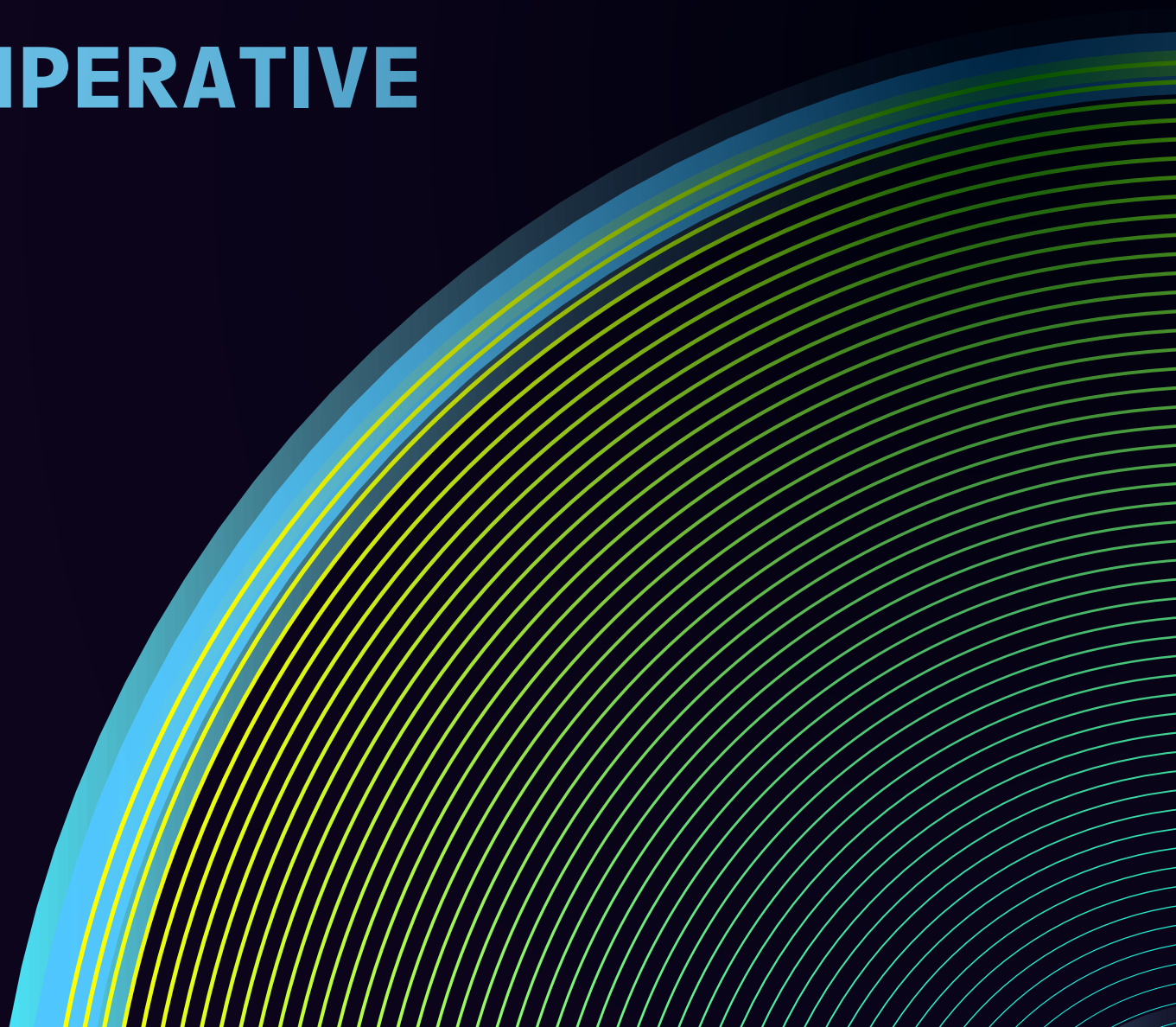
IGAP INDIAN GOVERNANCE AND POLICY PROJECT

EVENT REPORT
APRIL 2025

Symposium on:

AI, Dual-use Technology and National Security:

INDIA'S STRATEGIC IMPERATIVE



Index

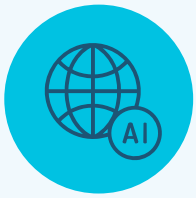
01 Introduction

The Symposium on **"AI, Dual-use Technology & National Security"**, organised by the Indian Governance and Policy Project ***(IGAP)*** and the Strategic Research and Growth Foundation ***(SRGF)***, was held on 29th April, 2025. It brought together officials from the Government of India, the Indian Armed Forces, senior representatives from leading technology companies, academicians, policy experts, and innovators from the deep-tech startup ecosystem. The Symposium aimed to generate actionable insights on the evolving intersection between Artificial Intelligence ***(AI)*** and national security within India's contemporary strategic environment.

Participants engaged in substantive discussions on how India can effectively navigate the multifaceted challenges and opportunities posed by AI in the realm of defence and security. A recurring theme throughout the deliberations was the recognition that AI is not merely a technological enabler but a transformative force with profound economic, political and military implications.

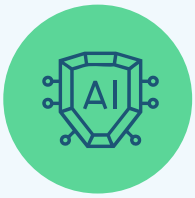
The Symposium was marked by a distinguished Welcome Address by Dr. Sasmit Patra, Member of Parliament, a Keynote Address delivered by Lt. Gen. MU Nair, National Cyber Security Coordinator, and a Valedictory Address delivered by Lt. Gen. Vinod G. Khandare, Principal Advisor, Ministry of Defence. Their valuable insights and contributions significantly enriched the discourse.

The event was structured around 4 key thematic sessions:



AI and Geopolitics: The New Global Battleground

AI Infrastructure and Compute Power: Ensuring India's Strategic Autonomy



AI, Dual-use Technology, and India's Defence Modernisation

AI Governance and National Security

This report is a synthesis of the principal discussions, key insights, and actionable recommendations that emerged from the Symposium. As the event was conducted under the **Chatham House Rule**; this report presents merely the substance of the deliberations in these sessions, without attribution to individual participants. It is intended to serve as a resource for policymakers, practitioners, and researchers, supporting informed dialogue and guiding strategic action in this critical domain.

02 Welcome Address

Dr. Sasmit Patra

Member of Parliament, Rajya Sabha

AI has already emerged as a defining determinant of national power in the 21st century. It is rapidly reshaping the geopolitical landscape—driving the formation of new global alliances, intensifying techno-nationalism, and accelerating the decline of unipolarity. What was once considered a dual-use technology is now becoming a default-use technology. Every commercial breakthrough in AI today finds near-immediate application in military, intelligence, and strategic domains. This shift carries profound implications for sovereignty, security, and the global order itself.

To navigate this transformation, India must urgently pursue strategic autonomy across all layers of the AI stack—data, compute, algorithms, and semiconductors. The country's semiconductor mission, therefore, must be viewed not merely as an industrial policy but as a national security imperative. The battle for compute capacity has become the new arms race. The struggle for algorithmic superiority and chip sovereignty will define future power equations.

We are also witnessing the emergence of an "AI iron curtain," as export controls and geopolitical restrictions create new technological boundaries. The democratisation of AI stands in tension with the concentration of AI capabilities in the hands of a few dominant actors. How we resolve this tension—through standards, regulation, and innovation—will shape both the ethics and power structures of the AI era.

We must therefore move beyond viewing AI solely through the lens of "AI for Good" and squarely engage with the strategic realities of "AI for Power." This entails asking how we build resilient and secure global AI supply chains, how we address regulatory arbitrage that threatens national security, and how we establish clear norms and guardrails for the use of AI in military and high-risk domains.

These are not just policy questions—they are national imperatives. As we deliberate today, let us do so with clarity and urgency. Because in the realm of AI, if we are not ahead, we are already behind.

03

Keynote Address: AI, National Security and India's Strategic Priorities

Lt. Gen. M U Nair (Retd.), PVSM, AVSM, SM

National Cyber Security Coordinator, National Secretariat (NSCS), Government of India

India's defence communications have evolved from basic physical communication lines to vast digital ecosystems. This transformation has fundamentally reshaped operational protocols, enabling significant force multiplication (i.e., enhancing the effectiveness and impact of military operations without a proportional increase in manpower or resources). Previously, the sheer volume of intelligence inputs overwhelmed human analysts. AI now mitigates this challenge by efficiently processing and extracting insights from large, multi-format datasets. Early recognition of AI's potential was evident in initiatives such as the establishment of the Centre of Artificial Intelligence and Robotics ***(CAIR)*** at Defence Research and Development Organisation ***(DRDO)*** in 1986.

AI's Dual-use Nature and Security Implications

As AI-generated data flows become ubiquitous, securing indigenous datasets is critical, as AI's performance depends on high-quality and diverse inputs. There is also an increasing complexity of security threats, ranging from machine-initiated attacks and disinformation campaigns to the mounting challenge of attribution in conflict scenarios. AI's impact on national security is profound, transforming the threat landscape with sophisticated, targeted, and highly scalable attacks—many of which are automated and difficult to trace, particularly in conflict and hybrid warfare.

Addressing AI Threats and Vulnerabilities

Specific threats are AI-driven information operation campaigns, supply chain vulnerabilities, and the potential compromising of encryption capabilities by advancements like quantum computing. These developments also raise significant ethical dilemmas regarding accountability and decision-making in AI-driven systems. While regulatory frameworks and numerous agencies

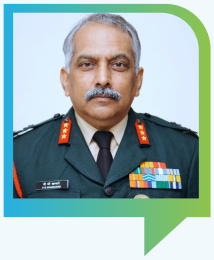
are engaged, the scale and sophistication of AI-driven threats pose significant complexity, making AI an integral and unavoidable component of national security requirements. Mitigating these pervasive threats demands strong international collaboration to secure the digital ecosystem.

There are vulnerabilities arising from large data repositories, risks associated with citizens leaving a large volume of digital footprint without adequate awareness, and weaknesses in service platforms and devices within India's vast digital ecosystem. A significant challenge also exists in terms of the low awareness among citizens regarding digital vulnerabilities and cyber hygiene, underscoring the urgent need to enhance citizen awareness at all levels.

Strategic Approach and Building a Secure Future

Building a secure and resilient future requires a multi-pronged effort. This involves developing mission-aligned AI solutions, securing robust indigenous datasets, and embedding ethical AI practices across all applications. Strengthening public-private partnerships is essential to mobilise resources and expertise effectively. A whole-of-society approach—bringing together citizens, industry, academia, and government—is vital to building enduring security and resilience in the digital ecosystem.

04 Valedictory Address: India's Defence AI Roadmap



Lt. Gen. Vinod G. Khandare (Retd.), PVSM, AVSM, SM
Principal Advisor, Ministry of Defence, Government of India

As digital technologies evolve at an unprecedented pace, they are transforming not only our infrastructure but also the landscape of national security. With every layer of digital expansion comes a broader surface for cyber threats—more sophisticated, more coordinated, and increasingly difficult to anticipate. In this context, it is vital to recognise the strategic imperative of harnessing technology not just as a tool of innovation, but also as a cornerstone of both defence and deterrence. Nations that fail to adapt risk being left vulnerable. Building resilience, therefore, demands the seamless integration of emerging technologies across all domains.

Role of Start-ups and Micro, Small and Medium Enterprises (MSMEs)

A recurring theme throughout the Symposium was the growing collaboration among government, private industry, and the start-up ecosystem. Startups are increasingly providing customised, context-specific solutions for national security and defence needs. However, the critical question remains:

> ***What solutions are relevant and necessary specifically for India?***

Answering this requires recognising that solutions effective elsewhere may not be appropriate in the Indian context. It underscores the need to foster domestic innovation that is tailored to India's unique operational and technological environment. This involves more than just funding—it calls for sustained demand through public procurement, enabling startups and MSMEs to scale viable, India-specific technologies.

Data Sharing and Trust

To ensure greater interoperability, the reluctance in data sharing needs to be addressed. This requires implementing secure data sharing practices and establishing Standard Operating Procedures ***(SOPs)***, data sharing protocols, and control mechanisms. These steps can ensure that data integrity and quality are not compromised and that innovators within the country are not deprived of essential resources.

Strategic Collaboration

Robust domestic innovation also depends on a well-connected defence innovation ecosystem. Greater cross-pollination among the armed forces and ministries, along with active engagement with the public and private sectors, is to be encouraged. India's defence diplomacy, and particularly the evolving role of defence attachés, is significant in this context. Their deployment is now guided by a strategic, data-driven process aimed at strengthening India's global presence in technology partnerships. With increased responsibilities and funding, defence attachés are now tasked with facilitating industrial collaboration abroad and enabling greater international outreach. This shift reflects a broader redefinition of diplomatic roles.

Need for Institutional Reforms

Finally, translating innovative solutions into operational capability requires enabling reforms in procurement and institutional frameworks. Reforms in defence procurement and capital acquisition must be prioritised to address long standing procedural challenges, notably lengthy timelines, and overly complex requirements. With reform efforts being actively driven at the highest levels, the focus must be on ensuring that procurement frameworks better align with operational requirements and strategic imperatives. This push requires a broader institutional recognition of the need for agility and transparency in defence acquisitions.

05 AI AND GEOPOLITICS: THE NEW GLOBAL BATTLEGROUND

This session explored the complex intersection of AI with geopolitics, focusing on its implications for national security, economic strategy, and global governance. Discussions highlighted both pressing risks and strategic opportunities, reflecting India's evolving position in the international AI landscape.

Assessing AI Risks to National Infrastructure

A key focus was the growing integration of AI into national infrastructure, particularly critical systems such as energy, finance, and defence. AI is significantly amplifying the capabilities of malicious actors by enabling cyberattacks that are more scalable, targeted, and adaptive. Generative AI can facilitate the creation of highly convincing phishing content and deepfakes, complicating detection and response mechanisms.

As these attacks evolve, tracing and attributing them becomes increasingly difficult. India must prepare for a landscape where AI-powered threats are countered by AI-driven defences, marking a shift towards an "AI versus AI" paradigm. This dual-use nature of AI, where the same technologies serve both attackers and defenders, highlights the imperative for India to build resilient, indigenous capabilities and infrastructure.

Defining Technological Sovereignty in the AI Era

The panel reframed technological sovereignty as a dynamic goal– not a binary choice between total dependence and complete self-sufficiency. Building domestic capabilities while partnering with trusted global partners was viewed as the practical path forward. Drawing parallels with defence acquisitions such as Rafale and MiG fighter planes, it was noted that complete domestic ownership is not always necessary; trust-based partnerships can also uphold sovereignty.

However, safeguarding national interests demands rigorous oversight of technology and data sharing, especially in defence and critical infrastructure. To maintain strategic autonomy, India

must focus on foundational pillars such as compute infrastructure, data governance, and homegrown algorithm development. The accelerating pace of AI advancement also underscored the need for continuous investment and adaptive capacity-building to prevent obsolescence.

Data Colonisation and Sovereignty Risks

'Data colonisation', i.e., the unchecked accumulation of vast user data by foreign entities, was flagged as a growing risk, creating vulnerabilities in privacy, control, and sovereignty. Examples such as apps that gather personal data through entertainment features (e.g., *Ghibli-style* image generators) illustrate how dependencies can form quietly. The discussion also highlighted the Digital Personal Data Protection ***(DPDP)*** Act, 2023, and the potential role of the India Data Management Office in strengthening data governance and ensuring robust public datasets to counteract external dependencies.

Strategising India's Engagement in the International Trade Scenario

This session stressed the importance of India establishing its own clear benchmarks and sovereign priorities before deepening global engagements. Today's geopolitical environment requires a holistic economic security strategy that addresses supply chain resilience, sustainable growth, and the balance between external and domestic economic drivers.

While acknowledging historical challenges in manufacturing and hardware development, recent industrial policy shifts were found to be promising. Rather than comparing India's pace of industrialisation to early adopters, participants emphasised identifying niche areas for leadership, recognising that technology is dynamic and constantly evolving. Participants noted that while multilateral platforms (like G20 and BRICS) are valuable, regional and bilateral collaborations—such as the Quad and Indo-Pacific Economic Framework ***(IPEF)***—may offer more focused outcomes.

1

The **Quad** is a diplomatic partnership between Australia, India, Japan, and the United States committed to supporting an open, stable and prosperous Indo-Pacific that is inclusive and resilient.

2

The Indo-Pacific Economic Framework (IPEF) is a non-binding framework for economic cooperation and connectivity in the Indo-Pacific region, while the Quad is a security and strategic dialogue platform.

Strategic Collaboration in Research and Development

While international collaboration is essential for advancing AI capabilities, the growing concerns over foreign entities gaining access to India's strategic and sensitive technological developments was highlighted. A notable trend discussed was the rising presence of foreign funding in Indian startups—often aimed at acquiring 'incremental IP' that reflects the nation's emerging technological edge.

At the same time, with major powers accelerating their R&D ecosystems through aggressive investment and international alliances, India cannot afford strategic isolation. Keeping pace with global innovation trends may necessitate carefully structured partnerships. This dual reality underscores the need for a deliberate and calibrated approach—one that enables India to benefit from collaboration while protecting critical IP and maintaining technological sovereignty.

Preparing for the Quantum AI Frontier

Quantum computing, particularly when merged with AI, was identified as a significant future frontier with profound security implications, citing China's progression in quantum computing with the Zuchongzhi 3.0 processor. The potential for quantum AI systems to break current encryption standards poses a major concern, prompting nations like the United States ***(U.S.)*** to ask its agencies to explore post-quantum cryptography. While presenting challenges, quantum AI also represents an opportunity if strategic investments and research are undertaken.

3

The Zuchongzhi 3.0 is a powerful quantum processor built in China with 105 qubits. It showcases the ability to solve a complex problem in just a few seconds, something that would take the world's fastest supercomputers over 6 billion years.

Promoting Responsible and Inclusive AI

India's Digital Public Infrastructure ***(DPI)*** was discussed as a successful model for leveraging technology for the public good and inclusion. Initiatives like Bhashini, focused on language translation, as prime examples of how AI integration at scale can deliver services effectively and promote social good. This approach could serve as a foundation for developing and deploying AI solutions specifically tailored to India's unique socio-economic context. India's skilled workforce and DPI framework position the country well for developing ethical, impactful AI systems.

Export Controls, AI Democratisation, and Strategic Sovereignty

The panel discussed the shifting relevance of traditional export control regimes in the context of AI's rapid global diffusion. It was noted that traditional models are less effective in constraining such regimes and have limited success in curbing the spread of advanced AI capabilities. The example of DeepSeek R1's development in China, despite U.S. export restrictions, illustrates the resilience of AI ecosystems to containment efforts.

This discussion intersected with concerns around AI democratisation and the rise of sovereign AI models. The stark price difference between OpenAI (USD 15) and DeepSeek R1 (USD 0.5) for similar input-output token use was noted as a marker of shifting global dynamics. Participants highlighted that the interplay between proprietary and open-source AI models presents complex strategic choices—on one hand, enabling broader innovation and access, while on the other raising risks around rapid market dominance and national security vulnerabilities.

While open-source models can accelerate innovation and lower entry barriers, they also increase the risk of misuse, particularly in adversarial contexts. The panel emphasised the need for a measured approach that balances the benefits of open access with the imperative to safeguard strategic interests and prevent unintended consequences.

India's Global Leadership and Approach to AI Governance

India has consistently championed the principle of 'AI for Good and AI for All' in international forums, including through its role as a founding member of the Global Partnership on AI. This position reflects a commitment to ensuring that AI development is inclusive, equitable, and aligned with broader human development goals—particularly across the Global South.

Building on this global stance, the panel noted that India was well-positioned to adopt a balanced governance framework—one that supports innovation, enables startups to thrive, and avoids overly restrictive measures that could hinder technological growth.

Observing contrasting global regulatory models—the more innovation-driven, open-ended stance of such as the U.S. approach prioritising innovation, and the European Union's stricter, risk-based regulatory regime—participants emphasised the need for India to chart its own path. This would involve calibrating oversight to national priorities while actively enabling the development of domestic AI capacity.

06 AI INFRASTRUCTURE AND COMPUTE POWER: ENSURING INDIA'S STRATEGIC AUTONOMY

This session examined the evolving understanding of AI, beginning with its contested definitions and moving toward strategic questions of sovereignty, partnerships, and infrastructure. Anchored in the national security context, the session explored how India might shape its AI trajectory through collaborative models and efficient compute deployment.

Sovereignty through Control or Commons

AI should not be viewed as a standalone product, but as part of a broader ecosystem. This includes cloud infrastructure, data centres, high-end semiconductors, models of various scales, and training datasets. In this context, a realistic degree of Indian strategic autonomy across these layers requires consideration. The panel presented varying views on this particular point. One perspective emphasised that sovereignty must encompass end-to-end autonomy across all the layers of AI. A key challenge in this regard is the choice between commoditisation and proprietary control of AI. Certain layers of the AI stack, such as large language models ***(LLMs)***, middleware, and cloud infrastructure, are gradually becoming commoditised, making them more accessible and replicable. While other components, such as high-quality datasets, remain under tight proprietary control, making them inherently difficult to reproduce.

It was discussed that the rise of agentic AI, like AI assistants, signified the importance of proprietary control, while emerging developments like DeepSeek marked a shift towards commoditised models. Therefore, achieving sovereign AI may not require complete proprietary control from the start; instead, countries can choose which layers to develop domestically and where to collaborate, depending on national priorities and available capacity.

Balancing Control and Collaboration

Another perspective emphasised the lack of domestic control over several critical AI components that run within these layers, which is a key challenge to achieving end-to-end autonomy in AI. While India has made rapid progress in building data centres, core elements of AI platforms like

application programming interfaces ***(APIs)***, access control systems, and cryptographic tools are not domestically owned or operated. Even foundational technologies such as atomic clocks, which are essential for synchronising AI systems, rely on foreign systems like GPS. Drawing on the example of the Kargil conflict, where India lost access to GPS due to foreign control, it was stressed that strategic infrastructure such as hardware and compute capacity must be developed indigenously over time.

In order to build such strategic infrastructure, the high 'cost of compute' was identified as a major barrier. India's current fiscal and technological capabilities act as constraints in this domain. This has resulted in the need for international collaborations in the near term. However, the panel emphasised the importance of maintaining domestic control over critical systems, particularly those related to national security, defence, and essential public services—even while engaging with global innovation networks. 'Middleware' was also recognised as a key enabler, without which large-scale enterprise and public deployment would remain limited.

4

Middleware - Middleware creates a secure link between the app and the data it needs. It also checks if the user is allowed access by asking for things like a username, password, or digital certificate.

Exploring Public-Private Partnerships as a Solution

Due to resource constraints and the capital-intensive nature of AI infrastructure, strategic prioritisation of specific uses was seen as essential. This includes clarifying the government's role in developing critical capabilities. While strong incentives are considered necessary, it was recognised that they are insufficient without assured demand and mechanisms for risk-sharing.

When technologies are developed for national security and defence-adjacent applications, they may effectively be air-gapped from commercial markets. In such cases, the commercialisation of proprietary technologies may still be pursued by private firms, but clear commercial pathways for government-funded solutions are not always guaranteed. To address this, it was suggested that demand be created by the government through procurement, deployment, or ecosystem-building, so that strategic investments in AI infrastructure and defence-related technologies are rendered viable and sustained.

An optimistic outlook was expressed for Indian data centres and cloud infrastructure, with organic growth already being observed. It was noted that, with supportive policies, further expansion could be achieved by both domestic and multinational companies, driven by rising demand from digital adoption. India's model of public-private partnerships ***(PPPs)*** was

highlighted with examples such as the Unified Payment Interface ***(UPI)*** and the Open Network for Digital Commerce ***(ONDC)***, cited as successful instances. The success of initiatives was attributed to open standards, transparency, and accessibility. However, it was cautioned that not all PPP models had been successful. For instance, in telecom infrastructure, poor risk-reward distribution was seen to contribute to failures. Consequently, it was recommended that future AI-related PPPs should be designed to ensure a reasonable distribution of risks and rewards. The discussion on PPPs concluded with the suggestion that private and global collaboration should be encouraged where appropriate, while long-term self-reliance continues to be pursued.

Optimal Compute Utilisation

It was argued that AI cannot function without strong cloud adoption, signalling that compute power was not just reliant on hardware, but the organisation, storage, and processing of data. Therefore, to use AI effectively, India needed structured data strategies, cloud-based storage, and the ability to process data at scale.

Cloud service providers, especially global hyperscalers, have played a key role in building digital infrastructure across the Global South, including India. Therefore, rather than focusing entirely on building every layer of the AI stack from scratch, a view expressed was that India can lead competitively if it leverages its resources and partnerships. It was suggested that India, with its rapidly growing talent base, can attract investment and drive innovation. The IndiaAI Mission was cited as a good example of this approach. The initiative to increase GPU capacity from approximately 15,000 to 29,000 units was achieved through effective public-private collaboration, including participation from both Indian and international companies.

Finally, India should balance strategic control with smart collaboration, while also reducing long-term dependencies. Therefore, the immediate priority would be to leverage available compute resources through cloud adoption, ecosystem partnerships, and efficient infrastructure planning.

07 AI, DUAL-USE TECHNOLOGY, AND INDIA'S DEFENCE MODERNISATION

This session examined the evolving role of AI as a form of dual-use technology in India's defence modernisation. It addressed AI's transformative potential, ethical dilemmas and operational risks. The discussions spanned from civil-military fusion and indigenous capabilities, human oversight, to sovereign AI defence strategy.

Dual-use in the AI Era

The future of India's defence modernisation is being shaped by the dual-use nature of AI and emerging technologies. In the past, technology was often transferred from the defence sector to civilian domains, with developments such as the internet and computing emerging from government-sponsored programmes. Technological innovation is now being led by the civilian tech sector, which is evolving at a pace faster than traditional defence development. This was seen as especially true for commercial applications of technologies like AI and quantum computing. Further, civilian technologies like AI are rapidly being adapted for military use, evident in recent conflicts such as those in Ukraine and Israel. India, therefore, needed to prioritise the development of its own military-grade AI systems with higher levels of autonomy. Because of the risks discussed earlier, it was suggested that India should carefully choose which AI capabilities to develop on its own and where to work with other countries. Since AI can be used for both civilian and military purposes, it offered a way to modernise by combining efforts across both sectors.

AI in Defence: Applications, Ethics, and Contextual Requirements

While commercially developed tools like ChatGPT, DeepSeek, and Grok demonstrate advanced capabilities, they remain unsuitable for critical military decision-making, where precision, reliability, and trust are paramount. It was argued that defence applications demanded stricter evaluation and oversight, especially given the potentially significant consequences of erroneous decision-making. This creates an impetus for India to build its own capabilities and research infrastructure for using AI in the military appropriately.

AI is widely used in logistics and training, but its use in direct combat was viewed by some participants as 'limited' due to ethical and practical concerns. The ethical implications of Lethal Autonomous Weapon Systems ***(LAWS)***, particularly the ethical control and delegation of life-and-death decisions to a machine, are being actively discussed internationally by the United Nations Group of Governmental Experts ***(GGE)***, with a draft international legal text expected by 2026. India's current stance has been one of strategic caution, engaging in discussions while refraining from firm commitments, allowing flexibility amid a rapidly changing landscape.

At the same time, the session highlighted that edge and agentic AI offer new opportunities, especially in areas like electro-optics and targeting. Speakers emphasised that AI systems for defence should be customised to suit India's varied terrain and operational needs, such as high-altitude regions and counter-terror operations.

Relevance of Human Oversight

Addressing the inherent risks of deploying AI in defence, particularly in critical systems like LAWS, the session underlined the necessity of human oversight. Unlike deterministic systems, AI's non-deterministic behaviour and unpredictable errors complicate risk assessment and may warrant stringent human oversight. The discussion highlighted differing interpretations of "human in the loop" or "human on the loop"- ranging from active decision making to passive oversight.

5

'Human in the loop' refers to the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable.

6

'Human on the loop' refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation.

This raised a broader question: what level of risk is societally acceptable? While no system is infallible, it was acknowledged that the acceptable level of risk would ultimately depend on the specific context in which the AI is deployed and the potential consequences of failure. Accordingly, oversight mechanisms must be proportionate—more stringent in high-risk applications and appropriately flexible where the stakes are lower.

Navigating the Challenges of Data Sharing

From a military standpoint, concerns around data sharing for AI training were noted. To address this, privacy-preserving techniques such as homomorphic encryption and synthetic data were suggested. The discussion also highlighted the need to prepare for emerging quantum threats, such as sensitive data retrieval, and the importance of technologies that enable cryptographically verified data deletion.

While addressing data challenges, it was noted that data generated by modern systems like drones would be of little value if it lacked depth or precision for specific military use cases. The panel also recommended upgrading older systems to enable the collection of relevant and higher-fidelity data.

Discussions highlighted the ethical imperative to resolve the weaponisation of lethal AI through international legal frameworks. It was also emphasised that military AI, unlike general AI, necessitates structured, trustworthy data tailored to specific use cases, prioritising data relevance, context, and model features over quantity due to the risk of data obsolescence. Proposed measures included establishing mechanisms for controlled external knowledge inflow while strictly preventing sensitive data outflow, acknowledging AI's potential to reduce military personnel's cognitive load.

Key Pillars of India's AI Defence Strategy

India's strategic approach to AI in defence must be fundamentally use-case driven, ethical, and forward-looking. Developing indigenous data ecosystems, fostering domestic models, and building national talent pipelines would be essential for ensuring long-term security and autonomy in this field. It was therefore suggested that AI regulation must be context-sensitive, as the risks and implications vary widely by application. For example, the factors impacting facial recognition used for access control differed significantly from those affecting its use in surveillance, or targeting.

08 AI GOVERNANCE AND NATIONAL SECURITY

This session examined the evolving role of AI as a form of dual-use technology in India's defence modernisation. It addressed AI's transformative potential, ethical dilemmas and operational risks. The discussions spanned from civil-military fusion and indigenous capabilities, human oversight, to sovereign AI defence strategy.

Innovation and Regulation: Striking a Balance

A central theme of this session was the longstanding tension between regulating emerging technologies and enabling innovation. The panel echoed the view that regulation must enable, not pre-empt, innovation, with the idea that 'innovation should lead, regulation will follow'. Concerns were raised about overly prescriptive frameworks. The European Union's General Data Protection Regulation ***(GDPR)*** was cited as an example, with discussions in the European Union increasingly recognising the need to ease compliance burdens on Small and Medium Enterprises ***(SMEs)***.

While India's current 'light-touch' approach to AI regulation was acknowledged, participants called for greater policy clarity, emphasising that regulatory ambiguity can deter investment and hinder long-term planning.

Rather than a single overarching AI law, sector-specific regulation was discussed as a practical alternative. This approach allows regulators to apply domain expertise in addressing AI's unique impacts. However, current frameworks were seen as inadequate in handling AI-specific legal grey areas, such as proprietary rights over training data. For instance, India's Copyright Act, 1957, does not clearly address whether training LLMs on copyrighted material constitutes infringement. These gaps underscore the need to modernise existing laws to reflect the realities of AI development and deployment, ensuring legal certainty while enabling innovation.

Re-thinking Self-Regulation

As part of the broader discussion on AI governance, another perspective offered was the role of self-regulation as a flexible and adaptive approach. Seen as a potential middle ground, it could bridge the gap between rigid compliance frameworks and the risks of complete deregulation. This viewpoint emphasised that, while self-regulation can support innovation and foster industry responsibility, it must be underpinned by clear standards to ensure accountability and public trust. The example of the U.S. Executive Order 14110 was cited—highlighting that, although intended to promote safe and trustworthy AI, its mandatory compliance obligations were viewed by some as overly prescriptive and potentially stifling to innovation. This raised the question of whether industry-led, principles-based approaches might offer a more agile alternative, particularly in rapidly evolving technological domains.

Context-Driven, Risk-Based Regulation

It was argued that AI regulation should focus not on the technology itself, but on its specific use-cases. Risks stem not from AI inherently, but from how and where it is deployed. A context-driven, risk-based approach—particularly important in high-stakes sectors such as finance, defence, and autonomous systems—was seen as essential for responsible governance.

In defence and national security applications, this distinction becomes especially critical. AI tools are deployed across core functions like command, intelligence, surveillance, and threat detection, where the consequences of error are severe. Conventional fairness metrics suited to civilian domains may not apply here. For instance, bias in classification systems may lead to the wrongful identification of individuals as combatants based on attributes such as gender—posing serious legal and ethical risks. This highlights a fundamental difference from acceptable differentiation in civilian contexts like healthcare. Rather than aiming for universal fairness standards, the emphasis should be on mitigating biases that compromise operational effectiveness and decision accuracy.

To support the ethical and responsible deployment of AI, a structured, risk-based regulatory framework was recommended. Applied across the AI lifecycle, such a framework would help identify, assess, and mitigate risks while ensuring transparency, fairness, and safety. Crucially, transparency requirements should be proportional to the level of risk and contextual factors, placing appropriate obligations on all actors involved in the AI ecosystem.

Threat Actors and the Need for Collaboration

A major concern was the growing collaboration between nation-state actors and cybercriminals in launching sophisticated, AI-enabled attacks. This blurring of lines between state and non-state actors calls for greater international cooperation among governments, regulators, and technology companies to build collective resilience.

Institutional Readiness for Responsible AI

To foster innovation and build public confidence in AI systems, the establishment of clear accountability and trust-building frameworks was deemed essential. Systemic risks posed by AI must be met with appropriate guardrails that impose responsibility on all actors across the development and deployment pipeline. A framework rooted in transparency, fairness, explainability, and accountability would play a critical role in ensuring the ethical use of AI and cultivating citizen trust.

In parallel, the need to build technical competency—particularly within regulatory institutions—was underscored. The proposed Indian AI Safety Institute is envisioned as a key step in this direction. By identifying and mitigating AI-related risks, maintaining an AI Incident Database, evaluating models, and fostering international collaboration, such institutions could help operationalise AI governance frameworks and ensure their long-term sustainability.

Greater Interoperability

Regulatory harmonisation was seen as necessary, particularly in the context of reporting attacks, given the intertwined nature of cyber and AI-enabled attacks. Divergent cyber incident reporting norms, observed across various sectoral regulators with differing timeframes and formats, highlighted a key area ripe for harmonisation.

Contrasting perspectives were also presented, emphasising that not all AI incidents are confined to the cyber domain, as AI applications can extend into the physical realm. This distinction stressed the need for an 'AI Incident Database', which could provide insights into AI incidents across contexts, aid in identifying high-risk systems, and support risk and impact assessment.

09 Key Takeaways

Need for a Risk-based and Contextual Approach

AI governance requires a risk-based approach to identify and mitigate risks throughout the lifecycle. It must also be contextual, tailoring standards like fairness and transparency to specific use cases, particularly in national security, where universal rules may not apply.

Enhancing Interoperability

Achieving greater interoperability is crucial within the AI governance landscape, particularly through enhanced coordination between the emerging AI governance framework and existing sectoral regulations.

Pursuing Sovereignty in the AI Age

Technological sovereignty for India in the AI era is strategically defined not by self-sufficiency, but by blending robust domestic capability building with trusted global integration and collaboration.

Addressing Challenges within the Data Ecosystem

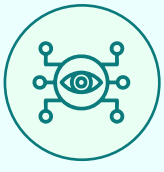
Despite the enormity and strategic importance of data across India's digital ecosystem, significant challenges persist, particularly regarding citizen awareness of digital vulnerabilities and data leakage. Given these challenges, ensuring data security, control, and fostering reliance on indigenous datasets is critical.

Public-Private Partnerships

Strategic AI development in India, particularly for defence capabilities and critical infrastructure, requires robust public-private partnerships that secure assured demand, enable equitable risk-reward sharing, and foster domestic innovation.

Strategic Integration for Resilience

A nation must strategically integrate technology across domains for both offensive and defensive capabilities to ensure resilience amidst the evolving nature of cyber and AI-enabled threats.



Human Oversight in Defence AI

Given the inherent risks of AI in critical defence systems, appropriate human oversight should be ensured and needs to be calibrated to context and potential impact.

Sustaining Thought Leadership

The geopolitical impact of AI underscores the need for sustained thought leadership focused on developing indigenous capabilities, promoting AI for the common good, and ensuring supply chain resilience.

Endnotes

1. Australian Government, 'The Quad' *(Department of foreign Affairs and Trade)*.
   https://www.dfat.gov.au/international-relations/regional-architecture/quad

2. Ministry of Commerce and Industry, 'India signs first-of-its-kind agreements focused on Clean Economy, Fair Economy, and the IPEF Overarching arrangement under Indo-Pacific Economic Framework for prosperity' (*PIB Delhi* 22 September 2024).
   https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057489#:~:text=About%20IPEF,observer%20status%20in%20Pillar%2DI

3. Matt Swayne, 'Chinese Team Officially Report on Zuchongzhi 3.0, Claims Million Times Speedup Over Google's Sycamore' (*The Quantum Insider* 4 March 2025).
   https://thequantuminsider.com/2025/03/04/chinese-team-officially-report-on-zuchongzhi-3-0-claims-million-times-speedup-over-googles-willow/

4. Susnjara, S., & Smalley, I 'What Is Middleware?' (*IBM* 31 July 2024).
   https://www.ibm.com/think/topics/middleware#:~:text=Middleware%20typically%20establishes%20a%20secure,and%20password)%20or%20digital%20certificates

5. 'What is Human-in-the-Loop (HITL) in AI & ML?' *(Google Cloud)*.
   https://cloud.google.com/discover/human-in-the-loop

6. 'Human-on-the-loop in Machine Learning: What Is It and What It Isn't' (*Unidata* 26 September 2024).
   https://unidata.pro/blog/human-on-the-loop-in-ml/

10 ABOUT US

INDIAN GOVERNANCE AND POLICY PROJECT

The Indian Governance and Policy Project is an independent research initiative working at the intersection of policy, technology, markets, and India's national development. In an era shaped by rapid technological shifts, evolving security concerns, and changing global dynamics, IGAP produces actionable insights to help decision-makers navigate complexity with clarity and purpose. Our work is driven by a deep understanding of how state capacity, market forces, and emerging technologies interact in shaping India's strategic and developmental trajectory. We engage directly with the hard questions at the heart of India's future — from the governance of AI and digital public infrastructure to financial innovation, sustainability, and the evolving architecture of national security.

IGAP focuses on crafting solutions that balance India's legitimate security and developmental priorities with its democratic values and constitutional principles. We recognize that questions of governance today are inseparable from questions of technology, markets, and individual rights — and our research reflects that integrated reality. Through close engagement with governments, industry, technologists, and civil society, IGAP delivers research and strategic insight that is rigorous, relevant, and geared towards implementation. As a young and agile institution, we are committed to supporting India's leadership in building a secure, innovative, and inclusive future.

Website: www.igap.in | Email: relations@igap.in

STRATEGIC RESEARCH AND GROWTH FOUNDATION

The Strategic Research and Growth Foundation is a dynamic and emerging non-profit organization based in Pune, Maharashtra. Established in early 2023, SRGF is committed to advancing sustainable development, inclusive growth, and comprehensive national security. The focus is on three core areas: Social Impact, Capacity Building, and Policy Recommendations. By collecting first-hand, actionable insights, SRGF develops practical and effective strategies to address pressing national and humanitarian challenges.

Website: www.srgf.org | Email: info@srgf.org

EVENT REPORT | APRIL 2025

Symposium on: AI, Dual-use Technology and National Security: India's Strategic Imperative

SRGF
STRATEGY - RESEARCH - GROWTH

IGAP INDIAN GOVERNANCE AND POLICY PROJECT