EDITORIAL: THE HINDU

GENERAL STUDIES 3: SCIENCE & TECHNOLOGY **DATE: 18.04.2025**
TOPIC: ARTIFICIAL INTELLEGENCE

A closer look at strategic affairs and the AI factor

Context: Growing Concerns Over an AI Arms Race

- The rapid advancement of Artificial Intelligence (AI), especially toward the potential of Artificial General Intelligence (AGI), has triggered global debates about an AI arms race.
- AGI refers to AI systems that can **outperform human cognitive functions**, including solving problems beyond the scope of their training.
- While technical capabilities are being widely discussed, **strategic and policy-related discourse around AI remains underdeveloped**, leaving gaps in preparation for future threats.

Key Contributions and Debate

- A recent influential paper by **Eric Schmidt (former Google CEO)**, **Dan Hendrycks**, and **Alexandr Wang (CEO, Scale AI)** has attempted to address strategic challenges related to AI.
- The paper argues for **proactive state-led preparation** to handle security threats, especially if AGI becomes a reality.
- While some of their ideas—like AI non-proliferation—are constructive, others such as drawing parallels between AI and nuclear weapons face major conceptual flaws.

Questioning the Core Assumptions of the Paper

- One of the central proposals—**MAIM (Mutual Assured AI Malfunction)**—is modeled on **MAD (Mutual Assured Destruction)** in nuclear strategy.
- MAD implies that a nuclear attack by one country would invite an equally destructive counterattack, ensuring **mutual annihilation**, thus deterring war.
- However, MAIM is speculative and **does not replicate MAD's clarity or consequences**, since the nature of AI systems and their spread is vastly different from nuclear arsenals.
- This analogy risks leading policymakers into **over-militarized and misaligned AI strategies**, potentially escalating tensions unnecessarily.

Infrastructural and Conceptual Differences Between AI and Nuclear Technology

- Nuclear weapons are physically centralized, heavily regulated, and require specialized infrastructure.
- In contrast, AI projects are **diffused across global networks**, often involving open-source contributions and decentralised development.
- Destroying an AI project is **technically and logistically unfeasible** compared to targeting a nuclear facility.
- The idea of **preemptively sabotaging AI projects of rogue actors** could lead to **unintended escalation**, especially given imperfect surveillance capabilities and intelligence errors.

Concerns About Preemptive Action and Policy Consequences

- The paper's endorsement of sabotage or strikes on 'enemy' AI infrastructure raises serious ethical and strategic dilemmas.
- **Premature military action**, based on perceived AI threats, could violate international norms and worsen global stability.
- The **assumption that states can effectively monitor and destroy such projects** does not hold in the context of open, diffuse AI development environments.

Proposal to Control AI Chips: Another Flawed Analogy

- The authors propose restricting **AI chip distribution** in the same manner as controlling enriched uranium in nuclear non-proliferation efforts.
- This comparison is flawed because:
    - Once trained, AI models **do not require physical inputs** like uranium for continued function.
    - **Supply chain enforcement** is impractical in AI, especially as chips are used for multiple purposes beyond AI (e.g., gaming, graphics, computation).
    - Chips are globally manufactured and traded, making control difficult without **broad multilateral consensus**.

Speculative Assumptions and Gaps in Reasoning

- The authors assume that **AI-driven bioweapons or cyberattacks are inevitable**, but offer no concrete evidence.
- While AI can reduce the barriers to cyberattacks, **classifying it as equivalent to a Weapon of Mass Destruction (WMD)** is an overreach.
- They also assume that **AI development will remain state-led**, ignoring the fact that **private corporations currently lead most AI research**, only later adapted for national security by states.

- This underestimates the **commercial, civilian, and dual-use nature** of most AI technologies today.

Flawed Historical Comparisons: Strategic Errors in Thinking

- The use of **historical analogies from the nuclear era** may appear useful but risks oversimplifying the complex, decentralized, and non-kinetic nature of AI threats.
- Applying Cold War deterrence logic to AI can lead to policies that are **misguided, escalatory, or overly securitized**.
- Strategic frameworks built for centralized, physical weapons may not translate to **digital, evolving, and adaptable technologies** like AI.

Alternative Frameworks: The GPT Model

- Rather than nuclear analogies, AI can be better understood using the **General Purpose Technology (GPT)** framework.
- GPTs are technologies like electricity or the internet that **diffuse across multiple sectors** and reshape productivity, warfare, and governance.
- AI has not yet reached this 'general' threshold due to **limitations of current models (e.g., hallucinations, brittleness, narrow use cases)**.
- However, once matured, AI could become a powerful GPT—making **economic, industrial, and educational readiness** more important than deterrence-based thinking.

Need for Robust Strategic Scholarship on AI

- The current scholarship on AI in strategic and geopolitical affairs is **lagging behind its technical evolution**.
- Increased academic and policy attention is essential to:
    - Formulate **realistic frameworks for risk assessment**.
    - Understand AI's role in **asymmetric warfare, surveillance, and economic competition**.
    - Anticipate **unintended consequences of superintelligent AI**, if and when it emerges.
- Policymaking must be **informed, balanced, and forward-looking**, not based on outdated security doctrines.

Conclusion: Adopting Nuanced and Future-Oriented AI Strategies

- The idea of equating AI with nuclear weapons may attract attention, but **oversimplifies the unique risks and features of AI technologies**.

- Policymakers must avoid **copy-pasting deterrence frameworks from the Cold War**, and instead develop **context-specific, flexible, and collaborative models**.
- Investment in **international AI governance, public-private cooperation, AI ethics, and capability monitoring** will be key.
- Above all, **more thoughtful scholarship**—grounded in technical realities and geopolitical foresight—is needed to responsibly guide nations through the age of AI and AGI.

Source: https://www.thehindu.com/opinion/op-ed/a-closer-look-at-strategic-affairs-and-the-ai-factor/article69461728.ece