MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

AI and National Security: Major Power Perspectives and Challenges

Sanur Sharma

September 12, 2022

Summary

Advances in Artificial Intelligence will progressively multiply the threats, challenges, and opportunities from the national security perspective. Major Powers like the United States and China are investing big time in AI-enabled systems to enable them to maintain military lead. India is also taking steps in the field of military AI to be better prepared to face the future battlefield. Given the revolutionary implications for national security, the adoption of AI in the sphere of national security has its own challenges, spanning the ethical and regulatory realms.

Introduction

Artificial Intelligence (AI) is a stream of study that involves creation of advanced algorithms that can mimic the human brain. AI is often termed as a technology but instead it is an enabler to a constellation of technologies. The unique characteristic of AI is its potential to be integrated across various applications. AI's wide applicability in almost every sector has seamlessly permeated our lives—from the service sector (where we use voice assistants like Alexa, Siri, social media platforms, e-commerce websites, and Over-the-Top [OTT] platforms), to healthcare, agriculture, climate change, and the financial sector. In the defence sector, AI has immense potential for applications like Intelligence, Surveillance, and Reconnaissance (ISR), cyber security, military logistics, autonomous vehicles and Lethal Autonomous Weapons Systems (LAWS).

The past decades have seen an exponential increase in the adoption of AI in public and private sectors, which has been attributed to the increased computing power, explosion of structured and digitised data with cost-effective storage capabilities and advances in machine learning algorithms. The advances in machine learning models have abled machines to surpass human intelligence in specific functional areas. For example, the famous IBM Deep Blue defeated the world's number one chess champion, Garry Kasparov, in 1996. In 2016, Deep Minds Alpha GO defeated world champion Lee Seldol in the GO game. However, these systems involved many human inputs in training, testing and validation. To achieve general AI, there is still a long way to go where systems are capable enough to perform a broad range of tasks with human-level intelligence.

This Brief explores how major powers like the United States and China are leveraging AI to bolster their national security framework in order to maintain strategic advantage. It also flags India's efforts in the field of military AI and regulatory and ethical challenges associated with the dual-use application of AI.

AI and National Security

AI has attracted attention of policymakers and defence analysts because of its immense potential in the defence sectors. Recent developments in AI, for instance, have brought transformation in the domain of hybrid warfare.[1] The US National Security Commission on Artificial Intelligence (NSCAI) stated that AI "will be a source of enormous power for the companies and countries that harness them".[2]

[1] Greg Allen and Taniel Chan, "**Artificial Intelligence and National Security**", Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017.

[2] Christopher Gorman, "**Recent Developments in AI and National Security: What You Need to Know**", Lawfare, 3 March 2022.

The proliferation of AI is driving changes in the information domain, economic domain and military domain.[3] In information operations, AI has immensely enhanced capabilities for not only data collection but also advanced analysis and creation of data. AI-enabled systems have been widely used for image classification from drone footage, geospatial data analysis, audio and video analysis and detection of forgeries, and deep fakes.

Private investments in AI rose to US$ 93.5 billion in 2021, which is more than double the investments made in 2020 and the revenues are expected to surpass US$ 300 billion by 2024.[4] McKinsey estimates that AI has the potential to deliver additional global economic activity of around US$13 trillion by 2030.[5] AI has penetrated the private sector so seamlessly that almost every organisation today is either implementing AI into their systems and products or is planning to adopt it in their organisational architecture. It is being widely acknowledged that AI has the potential to start another industrial revolution where the population size will become less significant for national power.

In the military domain, AI is enabling new autonomous capabilities and making them affordable to a wide range of actors. The dual use of AI has given weak states and non-state actors more visibility and options to ramp up their capabilities. The use of AI in the cyber domain has led to the automation of various tasks, from advanced persistent threat operations to intrusion detection and prevention systems that are available for both offensive and defensive purposes.

The military potential of AI has transformed the nature of battlefields, with more autonomous systems coming into the security landscape. The interplay of this technology with the defence systems has enhanced asymmetric warfare options. There are diverse applications of AI in the military,[6] including in the area of ISR; Military Logistics; Cyber Space Operations; Information Operations and Deep Fakes; Integrated Command and Control; Semi-Autonomous and Autonomous Systems; and LAWS. The effective use of AI in applications in rockets, missiles, aircraft carriers, and naval assets and its integration in C4I2SR has made AI an essential factor in national security architecture.

[3] Greg Allen and Taniel Chan, No. 1.

[4] Daniel Zhang, Nestor Maslej, Erik Brynjolfsson, John Etchemendy, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Michael Sellitto, Ellie Sakhaee, Yoav Shoham, Jack Clark and Raymond Perrault, **“The AI Index 2022 Annual Report”**, AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, March 2022.; Neil Savage, **“Learning the Algorithms of Power”**, *Nature*, Vol. 588, 10 December 2020.

[5] **“The Global AI Strategy Landscape”**, Education Intelligence Unit, HolonIQ, 25 April 2019.

[6] **“Artificial Intelligence and National Security”**, Congressional Research Service (CRS), 10 November 2020.

Major Power Perspectives

Currently, more than 50 countries have published their National AI strategies to harness the benefits of this technology while addressing the challenges and risks associated with its fair use and governance. According to the Policy Note by Organisation for Economic Co-operation and Development (OECD), national AI policies of over 60 countries have been published.[7] Canada and Finland were among the first few countries to come out with their National AI strategies in 2017. Countries like the US and China have integrated AI into their military capabilities and enhanced their asymmetric means of warfare. The following sections will examine the efforts of the US, China in the field of military AI and place India's efforts in context.

United States

The US is investing heavily to develop "next generation air dominance" technology that could include sixth-generation fighters and drones.[8] Some examples include AI-based projects like Project Maven, Defense Advanced Research Projects Agency's (DARPA) Squad X Experimentation programme, and the OFFSET programme, which has been successfully deployed in Iraq and Syria to identify insurgents.[9] Military logistic software (IBM Watson software for predictive maintenance of aircraft and Ground vehicles—Stryker fleet)[10], cyberspace operations, autonomous vehicles like the Loyal Wingman programme (autonomous F-16), RCVs, and swarm drones are some other applications that the US is developing and deploying successfully. AI-enabled software like Clearview AI, SpaceKnow and Snorkel AI support federal efforts in identifying people, gathering geospatial data and analysing signals and adversary communications for high-value information, respectively.[11]

The US released its National Defense Strategy in 2018 that termed AI as one of the critical technologies that will ensure the US can fight and win wars in the future.[12]

[7] Laura Galindo, Karine Perset and Francesca Sheeka, **"An Overview of National AI Strategies and Policies"**, OECD Going Digital Toolkit Note, No. 14, 2021; Abhijit Akerkar, **"How AI is Advancing across the World Map"**, London Business School, 1 February 2019.

[8] The aim is an arsenal that "outpaces our competitors in the high-end conflict", said Navy Vice Adm. Ronald Alan Boxall, Director, Force Structure, Resources, and Assessment of the Joint Staff. See **"Comptroller Michael J. McCord and Vice Adm. Ron Boxall Hold a News Briefing on President Biden's Fiscal 2023 Defense Budget"**, U.S. Department of Defense, 28 March 2022.

[9] Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima and Derek Grossman, **"Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World"**, Research Report, RAND Corporation, 2020.

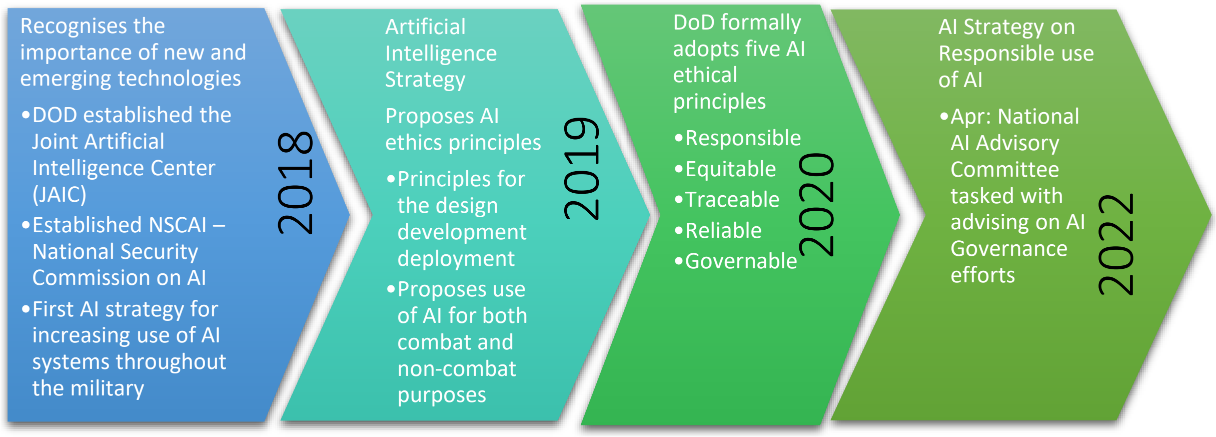
[10] **"Deploying AI in Defense Organizations: The Value, Trends, and Opportunities"**, Research Brief, IBM Centre for Business of Government, 2021.

[11] Paresh Dave and Jeffrey Dastin, **"Ukraine has Started Using Clearview AI's Facial Recognition during War"**, *Reuters*, 15 March 2022.

[12] **"Summary of the National Defense Strategy of the United States of America"**, U.S. Department of Defense, 2018.

In 2019, the US released its AI Strategy stating that “It is paramount for US to remain a leader in AI, to increase its prosperity and national security.”[13]

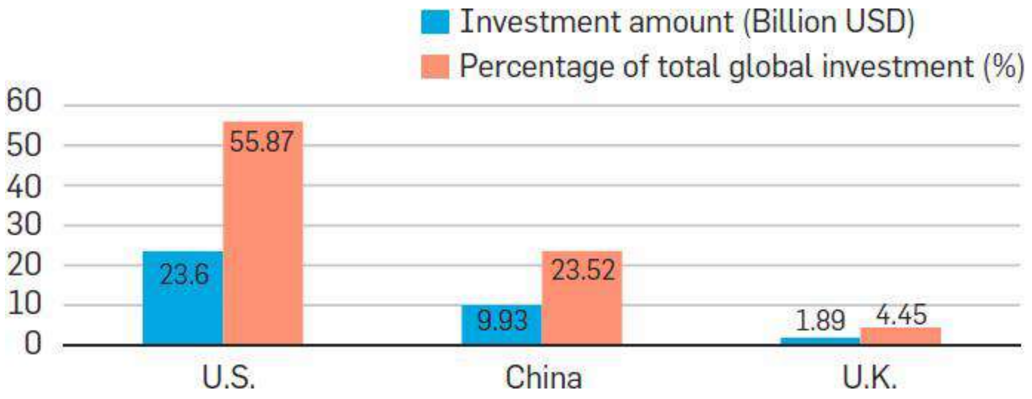
Figure 1. US AI Timeline


2018
Recognises the importance of new and emerging technologies
•DOD established the Joint Artificial Intelligence Center (JAIC)
•Established NSCAI – National Security Commission on AI
•First AI strategy for increasing use of AI systems throughout the military
2019
Artificial Intelligence Strategy
Proposes AI ethics principles
•Principles for the design development deployment
•Proposes use of AI for both combat and non-combat purposes
2020
DoD formally adopts five AI ethical principles
•Responsible
•Equitable
•Traceable
•Reliable
•Governable
2022
AI Strategy on Responsible use of AI
•Apr: National AI Advisory Committee tasked with advising on AI Governance efforts

Source: Author

The US Department of Defense plans to invest US$ 874 million this year in AI-related technologies as a part of the Army's US$ 2.3 million science and technology research budget. The Biden administration is requesting US$ 130 billion for the department's research, engineering, development, and testing budget for 2023, nearly 10 per cent up from last year's request. According to the AI index report of 2022, the US and China have dominated the cross-country collaborations on AI. Despite scrutiny of Chinese companies seeking partnerships or investments in the US, there are more Chinese investments in AI start-ups in the US than vice versa (See Figures 2 and 3).[14]

Figure 2. Comparison of the amount of investment in AI start-ups in the US, China, and the U.K. in 2020

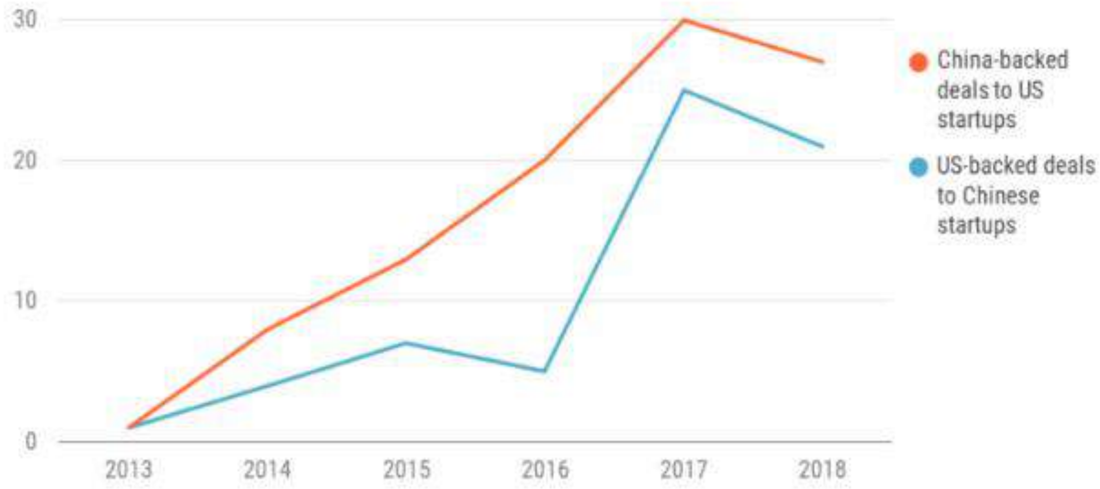


Source: Jaing Yang, “**AI Start-Ups in China**”, Communications of the ACM, November 2021, Vol. 64, No. 11.

[13] Terri Moon Cronk, “**DOD Unveils Its Artificial Intelligence Strategy**”, U.S. Department of Defense, 12 February 2019.

[14] “**China is Starting to Edge Out the US in AI Investment**”, CB Insights, 12 February 2019; Jing Yang, “**AI Start-Ups in China**”, Communications of the ACM, Vol. 64, No. 11 pp. 55–56, November 2021.

Figure 3. Cross- border AI deals continue despite scrutiny



***Source:* "China is Starting to Edge Out the US in AI Investment"**, Research Brief, CBInsights, 12 February 2019.

China

China is treading the path of military–civil fusion with PLA-supported AI developmental goals. It has made significant investments in Predictive Maintenance and Logistics, Information and Electronic Warfare, Command and Control systems, battlefield software, autonomous vehicles, training simulators and ISR systems. Some examples include the ASN-301 (a reverse-engineered copy of the IAI Harpy loitering munition), the GJ-11 "Sharp Sword" combat UAV, AI-based applications for leak detection, fault diagnosis, and 'smart warehouses' intended to predict and fill orders for material, AI-based knowledge mapping and combat decision support, among other capabilities. StarSee, one of China's military AI companies, successfully demonstrated tracking US naval assets in real-time off the coast of California in June 2020.[15] Due to China's lack of real-world combat experience, war gaming software have growing importance. AI-enabled war-gaming software like DataExa's AlphaWar (inspired by Deep Mind's AlphaStar) is used for professional military training.[16]

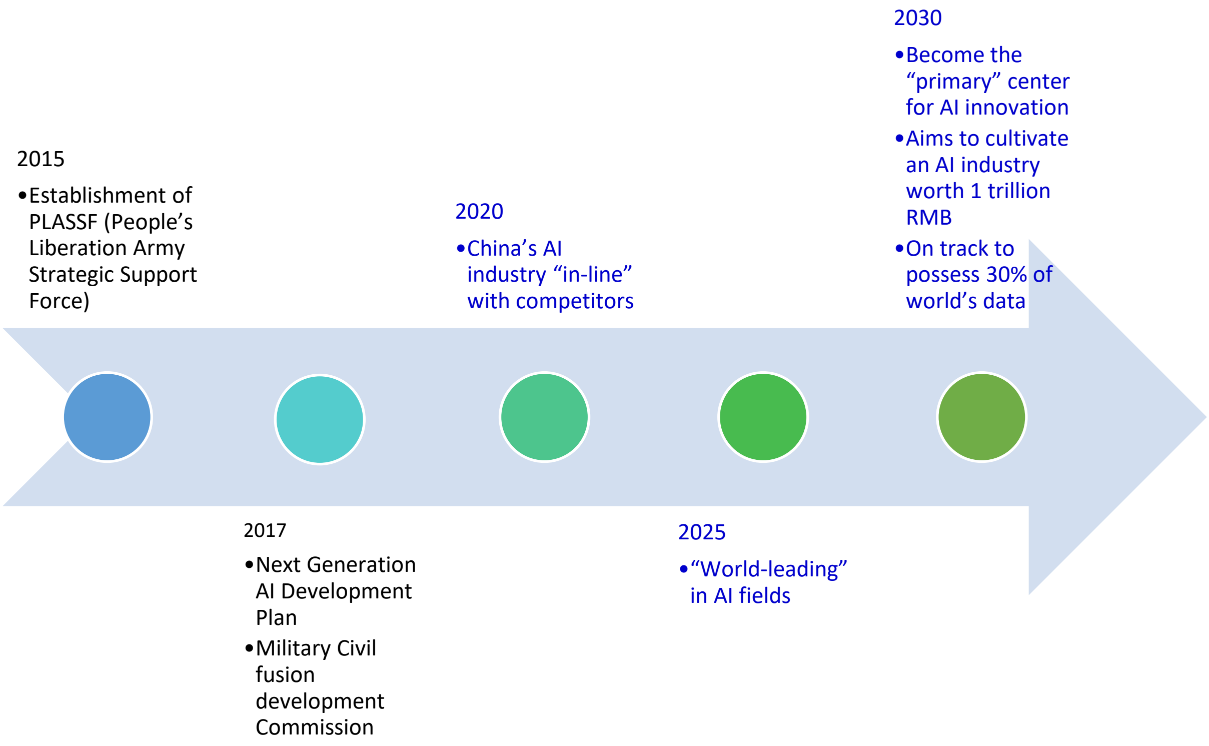
In addition, China in 2017 released a strategy detailing its plan to take the lead in AI by 2030. The establishment of PLASSF (People's Liberation Army Strategic Support Force) in 2015 and the New Era Roadmap in 2017 outline the complete AI ecosystem for the Chinese Army. According to its AI timeline, China is on track to

[15] Ryan Fedasiuk, Jennifer Melot and Ben Murphy, **"How the Chinese Military is Adopting Artificial Intelligence"**, Centre for Security and Emerging Technology, October 2021.

[16] Ibid.

become the "primary" centre for AI innovation to cultivate the AI industry worth 1 trillion RMB by 2030 (Figure 4).[17]

Figure 4. China AI Timeline


2015
•Establishment of PLASSF (People's Liberation Army Strategic Support Force)
2017
•Next Generation AI Development Plan
•Military Civil fusion development Commission
2020
•China's AI industry "in-line" with competitors
2025
•"World-leading" in AI fields
2030
•Become the "primary" center for AI innovation
•Aims to cultivate an AI industry worth 1 trillion RMB
•On track to possess 30% of world's data

Source: Author

India's AI Implementation Roadmap

India started its AI journey in 2018 when NITI Aayog came out with the National Strategy on AI.[18] However, it did not cover the Defence sector and was majorly for the commercial and private sectors (Agriculture, Healthcare, Education, Smart Cities and Infrastructure, Smart Mobility and Transportation). In the Defence sector, India can be seen as a late entrant but has been making decisive steps for matching up the major powers in terms of investment, indigenous development and bilateral and multilateral partnerships on the adoption of AI.

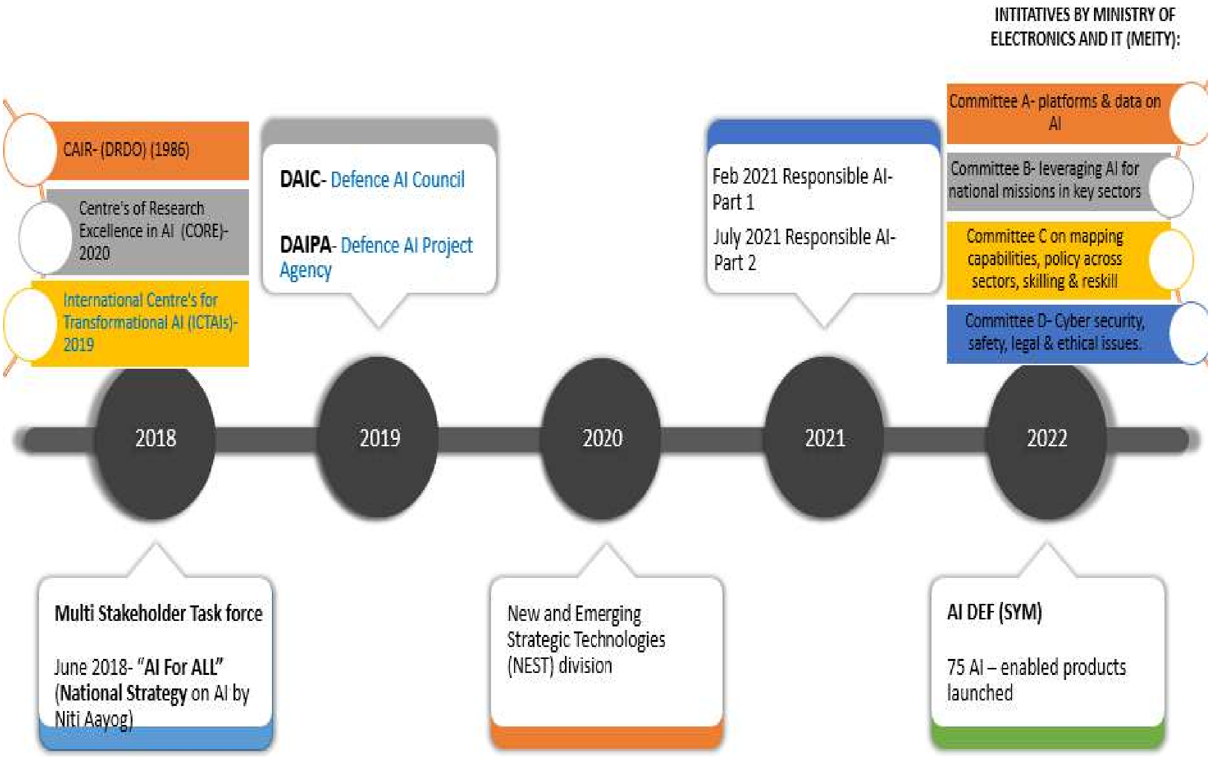
[17] Tim Dutton, "**An Overview of National AI Strategies**", *Politics+AI, MEDIUM*, 29 January 2018.

[18] "**National Strategy for Artificial Intelligence #AIFORALL**", NITI Aayog, 2018.

Defence AI Council (DAIC) and Defence AI Project Agency (DAIPA) have been constituted with Rs 1,000 crore annual budget specifically for AI-enabled projects.[19] Centre for AI and Robotics (CAIR), a laboratory of the Defence Research and Development Organization [DRDO], a primary laboratory for R&D in different areas of Defence Information and Communication Technology (ICT), is developing an AI-based Signal intelligence solution to enhance intelligence collation and analysis capabilities of the armed forces.

In July 2022, Ministry of Defence came out with 75 AI-enabled systems in the Def (Symp) specifically for the defence sector.[20] In addition, 140 AI-enabled sensor systems have been deployed across Pakistan and China borders.[21] The Indian Army will soon conduct trials of indigenously developed AI-enabled, un-crewed all-terrain vehicles in Ladakh for surveillance and logistics operations.[22]

Figure 5. India AI Timeline


INTITATIVES BY MINISTRY OF ELECTRONICS AND IT (MEITY):
CAIR- (DRDO) (1986)
Centre's of Research Excellence in AI (CORE)- 2020
International Centre's for Transformational AI (ICTAIs)- 2019
DAIC- Defence AI Council
DAIPA- Defence AI Project Agency
Feb 2021 Responsible AI- Part 1
July 2021 Responsible AI- Part 2
Committee A- platforms & data on AI
Committee B- leveraging AI for national missions in key sectors
Committee C on mapping capabilities, policy across sectors, skilling & reskill
Committee D- Cyber security, safety, legal & ethical issues.
2018
2019
2020
2021
2022
Multi Stakeholder Task force
June 2018- "AI For ALL" (National Strategy on AI by Niti Aayog)
New and Emerging Strategic Technologies (NEST) division
AI DEF (SYM)
75 AI – enabled products launched

Source: Author

[19] **"Task Force for Implementation of AI"**, Press Information Bureau, Ministry of Defence, Government of India, 28 March 2022.

[20] **"Raksha Mantri Launches 75 Artificial Intelligence Products/Technologies during first-ever 'AI in Defence' Symposium & Exhibition in New Delhi"**, Press Information Bureau, Ministry of Defence, Government of India, 11 July 2022.

[21] Ajay Banerjee, **"140 Artificial Intelligence-based Systems along Border to Keep Watch on China, Pak"**, *The Tribune*, 7 August 2022.

[22] Snehesh Alex Philip, **"Army to Conduct Trials of AI enabled Unmanned All-terrain Vehicles in Ladakh Next Month"**, *The Print*, 11 July 2022.

To develop cross-country linkages in the domain of AI and to lead technology diplomacy, the Ministry of External Affairs, Government of India in 2020 announced the New Emerging and Strategic Technologies Division. The US National Security Commission on AI in 2020 had stated that the US should form a US–India Strategic Tech-Alliance (USISTA) to develop Indo-Pacific Strategy on emerging technologies, considering India's increasing geopolitical standing.[23] The India–US 2+2 dialogue called for strengthening the bilateral partnership on emerging technologies.[24] At the QUAD Summit 2022, cooperation in the field of AI was flagged. India and Japan, in June 2022, also discussed essential areas of bilateral cyber cooperation and reviewed the progress in the areas of cyber security, ICT and 5G technology.[25] India and Finland have also agreed to work on areas involving new technologies like AI and quantum computing.[26]

Regulatory and Ethical Challenges

Given the revolutionary implications for national security, the adoption of AI in the sphere of national security has its own challenges. AI has brought disruption in the context of the changing landscape of security with the increased presence of hybrid warfare, cyber security threats like ransomware and the growth of technologies like Internet of Things (IoT). Cyber-physical systems have made it a complex affair. According to a report by Computer Emergency Response Team-India (CERT-In), India observed a 51 per cent increase in ransomware attack in first half of 2022 compared to the previous year.[27] In another report, it is suggested that by 2025, cyberattacks alone will lead to a loss of around US$ 10.5 trillion annually.[28]

Due to the dual use of AI (both military and civil applications), there is higher and easy accessibility of AI-based tools to non-state actors, which has further made it challenging to control the flow of technology. In addition, with the proliferation of social media, AI has become an inherent part of such platforms where it is being used to spread misinformation/disinformation, hate speech and radicalisation, further advancing national security threats.

[23] **"US Body on AI Calls For Creating India-US Strategic Tech Alliance"**, *Financial Express*, 14 October, 2020.

[24] Saroj Bishoyi, **"India-US Forging Tech Alliance Since Long. Now Use 2+2 Dialogue to Push it Further"**, *The Print*, 11 April 2022.

[25] **"India, Japan Discuss Cooperation in 5G Technology"**, *The Hindu*, 30 June 2022.

[26] T. Radhakrishna, **"Quantum Computing: India and Finland Agree to Set Up Virtual Centre of Excellence for Technical Cooperation"**, *The Economic Times*, 21 April 2022.

[27] **"India Ransomware Report H1-2022"**, CERT-IN, 2022.

[28] **"Cyber Security Statistics: The Ultimate List of Stats Data, & Trends For 2022"**, PurpleSec, 2022.

AI's extensive influence and success have the capability to alter the current power dynamics between nations. Furthermore, underfunded countries in AI may risk weakening their future military and economic dominance. For instance, despite the US$ 300 billion difference in the defence budgets of US and China, China is equally investing in AI as compared to the US.[29]

Key concerns on AI usage relate to ethical and regulatory issues. In the private sector, due to its easy availability and successful implementation, technology giants have control over the resources, which can easily lead to the weaponisation of AI. Authoritative nations like China are investing very heavily in such technologies and are deploying it against their own populations and even exporting such mass surveillance technologies to over 80 countries.[30]

Some concerning factors with ethical issues include data access problems as data availability or data openness is a crucial prerequisite for enablement of the AI ecosystem. Data protection regulations and protocols should be devised to promote specific open data sources for research to gain new insights from proprietary data. Biases in data like imbalanced datasets, racial issues and poisoning of data can considerably affect the efficiency of the AI algorithms and raise ethical concerns. For example, in image classification software, any discriminatory or biased information in the data can lead to inaccurate facial recognition.

Due to the black box nature or lack of transparency of AI algorithms, it becomes difficult for the decision-maker to understand the choice of the decision being made and raises concerns about the criteria used in automated decision-making, which further creates distrust regarding the use of such systems. Another issue that requires consideration is the lack of international regulation on developing and deploying AI-enabled weapon systems, including LAWS. It will enable great power competition between nations and escalate the arms race.

The question of accountability and liability is a discerning factor in cases where AI-enabled systems malfunction, where human lives are at stake. Therefore, it is indispensable to devise policies and standards that safeguard the use of AI systems. Accelerating efforts in the development of common standards and practices for the use, development and sale of AI systems will enhance better collaboration in digital space. There is an increasing debate on global platforms for devising regulatory frameworks and common standards, which is the right direction to make optimum use of advances in emerging technologies like AI.

[29] David Floyd, **"U.S. vs. China Military Spending: Which is Bigger?"**, Investopedia, 30 August 2021.

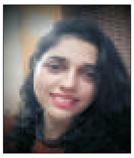
[30] Rohit Ranjan, **"US State Secy Blinken Asserts China Poses Serious Long-term Challenges To Int'l Order"**, *Republic World*, 27 May 2022.

Key Takeaways

Advances in AI will progressively multiply the threats, challenges, and opportunities from the national security perspective. The military potential of AI can be transformative as it can be a tool of weaponisation to automate weapon systems and enhance cyber warfare. Due to its dual use nature, multiple AI-enabled systems are available with state and non-state actors, making it a factor of concern for maintaining strategic stability and deterrence. AI governance, ethics, data bias issues and regulations are significant challenges in developing a thriving AI ecosystem.

Creating a supportive AI ecosystem in India will depend on investments in critical infrastructure, tapping the private sector innovation ecosystem and capitalising on the developments made by the leading nations in AI. It is essential to identify challenges and risks associated with this technology and build trust in AI through awareness, policy and regulations, and human resource development. Indigenous development will be a key in adding value to our defence systems, and so will the multilateral and bilateral partnerships towards adopting AI. These could span joint development of technology, technology sharing and partaking in global policy formulation and standardisation.

About the Author



Dr. Sanur Sharma is Associate Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Disclaimer: Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses