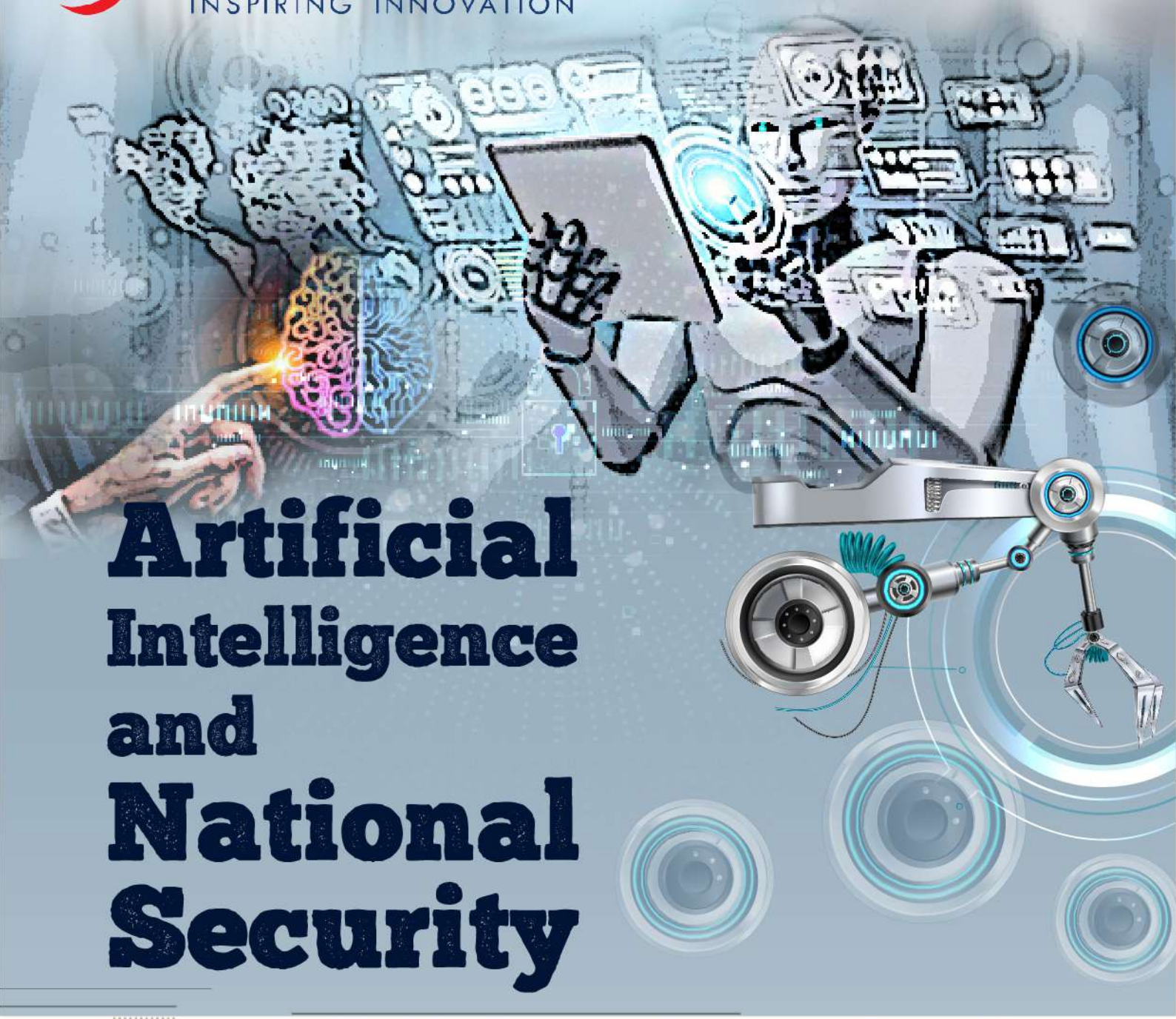


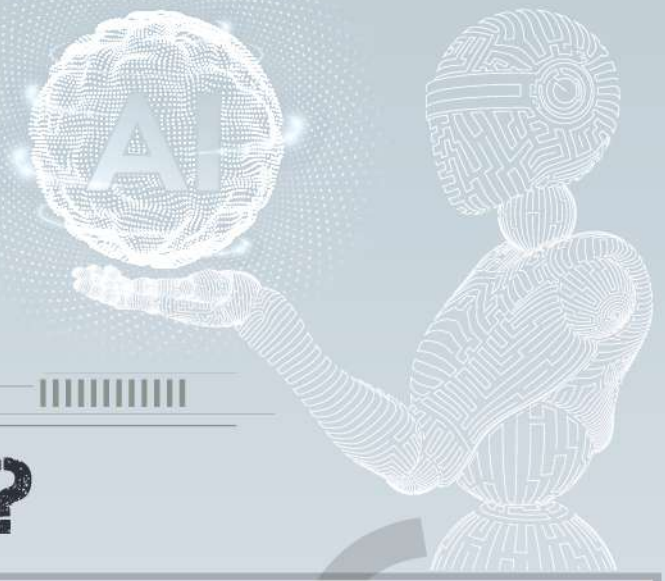
Artificial Intelligence and National Security

Introduction

Artificial intelligence (AI) is a rapidly growing field of technology that is capturing the attention of commercial investors, defense intellectuals, policymakers, and international competitors alike. Recently, developments like increased use of AI in cyberattacks and growth of hybrid warfare techniques have showcased how AI can potentially affect National Security.

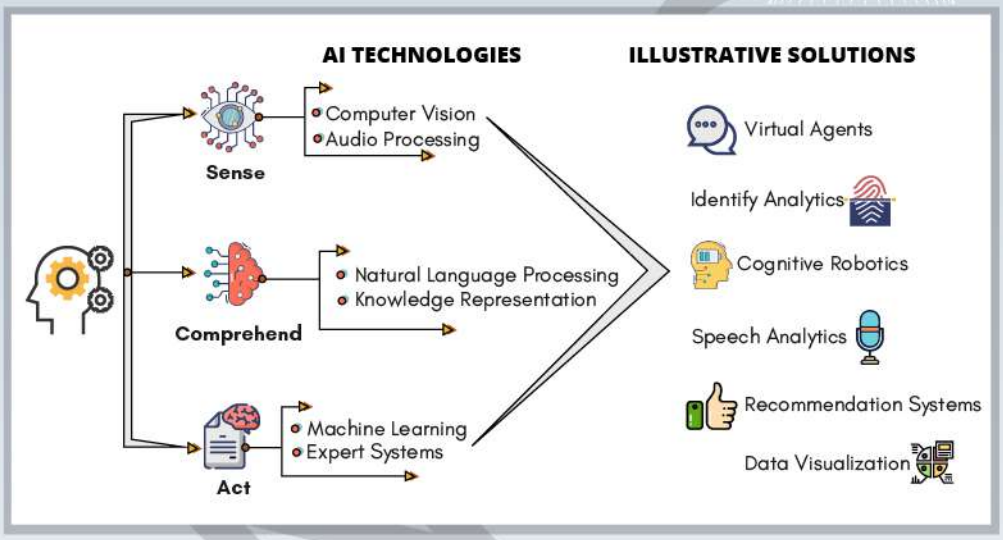
But what is Artificial Intelligence and how exactly is it relevant to National Security? If it is relevant, what are the opportunities AI can create to strengthen National Security? Will AI's penetration into national security alter the current global geopolitics? What has India done to tap the opportunities created by AI in National Security? What are the challenges in effectively utilizing these opportunities and what can be done to overcome these challenges? In this article, we will try to answer these questions.

What is Artificial Intelligence (AI) and how is it relevant to National Security?



AI refers to the **ability of machines to perform cognitive tasks** like thinking, perceiving, learning,problem solving and decision making. It can be considered as a constellation of technologies that enable machines to act with higher levels of intelligence.

The penetration of AI into our systems has recently exploded due to newer developments like **unlimited access to computing power, huge fall in the cost of storing data and explosion of digitized and structured data.**



At the same time, the domain of **national security has not been immune to the disruptions** caused by increasing use of AI. These disruptions can no longer be ignored in the following context:

- **Changing nature of security:** The traditional elements of security are rapidly expanding with technological developments leading to creation of newer challenges which are AI dependent.
  - **Increasing presence of Hybrid Warfare:** Both state and non-state actors are employing technology thus **making the dimensions of warfare multifaceted.**For example, the recent information theft by the China backed company Zhenhua can possibly threaten the internal security of the state by targeting key individuals.
  - **Rise in frequency and cost of cybersecurity threats:** Reports suggest that there was a **37% increase in cyberattacks** in Q1 of 2020 in India. This increase in frequency is accompanied by rising strength of malware and ransomware which proportionately increases the losses associated with cyberattacks. Some reports suggest that cyberattacks could **globally cost more than $5 trillion per year by 2024.** AI enabled tools have the potential to increase the defensive capabilities of security systems.
  - **Security is growing more complex:** Growth of continuous real-time connectivity, mobile platforms and Internet of Things (IoTs) in conjunction with Cyber-Physical systems has made the security landscape more complex. Integration of AI in the security architecture can help assess internal vulnerabilities as well as block internal threats.
- **Higher accessibility of AI based tools:** Earlier, the tools and technologies which had security implications like nuclear technology were by and large protected. This ensured that only limited actors had access to such technologies. But same cannot be said for AI because of:

- **Dual-use nature of AI applications:** Many AI applications are dual-use, meaning they have both military and civil applications. This makes **controlling the flow of such technologies extremely difficult.**
- **Absence of global coalitions for AI based tools on lines of Wassenaar Arrangement or Missile Technology Control Regime (MTCR):** In free flow of these tools across borders, all actors including rogue states and non-state actors can get access to these technologies. This may enable non-state actors to devise disproportionately large impacts from their operations. For example, interfering with Air traffic management systems.

- **Unavoidable presence of AI:** Artificial intelligence is now touching upon aspects of human life not only in economic domain but also in social domain. For example, **AI is integral part of technologies used by social media platforms** and can play an important role in overcoming national security threats like hate speech and radicalization on these platforms. Its presence gets further enhanced because-

  - AI has the **potential to be integrated across a variety of applications,** improving upon the "Internet of Things".For example, **AI can be incorporated into a system controlling hazardous chemicals** which can create a potential threat.
  - **Integration of AI into a product may not be immediately recognizable** i.e. it may not alter the physical structure of a system, but incorporation of AI, changes the overall functioning of the system. For example, it would be very difficult to decipher if a **drone is being controlled remotely or with an AI based system.**

While we have established how the growth of technologies (including AI) have altered the security landscape creating new challenges for our national security, these changes also simultaneously provide us with an opportunity to further strengthen it.

What are the opportunities AI can create vis-à-vis National Security?

AI, by virtue of its ability to mimic certain functions of human brain, when combined with adequate amount of resources can create opportunities like:

- **Increasing real-time intelligence:** AI is expected to be particularly useful in intelligence due to the **large data sets** available for analysis. Large scale structured data combined with the available computational power can generate **significant actionable intelligence.** For instance, it could be useful in accomplishing tasks like converting unstructured information from financial data to identify potential irregularities and security threats.

- **Creating autonomous and semi-autonomous systems:** These systems collectively increase the geographical reach of the military operations. For example, autonomous systems can be employed to further increase border security without endangering the lives of soldiers and can be incorporated in all major military vehicles including fighter aircraft, drones, ground vehicles, and naval vessels.

- **Lethal Autonomous Weapon Systems (LAWS)** are a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system.

- **Logistical ability:** AI may have future utility in the field of military logistics. For instance, it can ensure continuous observation of border infrastructure and provide intelligent inputs with respect to need for repairs.

- **Cyber operations:** AI is likely to be a key technology in advancing military cyber operations **both in offensive and defensive capacity.** For example, conventional cybersecurity tools look for historical matches to known malicious code, so hackers only have to modify small portions of that code to circumvent the defense. AI-enabled tools, on the other hand, can be trained to detect anomalies in broader patterns of network activity, thus presenting a more comprehensive and dynamic barrier.

- **Replacing humans in 'dull, dangerous or dirty' work:** Depending on the task, autonomous systems are capable of augmenting or replacing humans, freeing them up for more complex and cognitively demanding work. For example, AI can be used in conducting long-duration intelligence collection and analysis or cleaning up environments contaminated by chemical weapons.

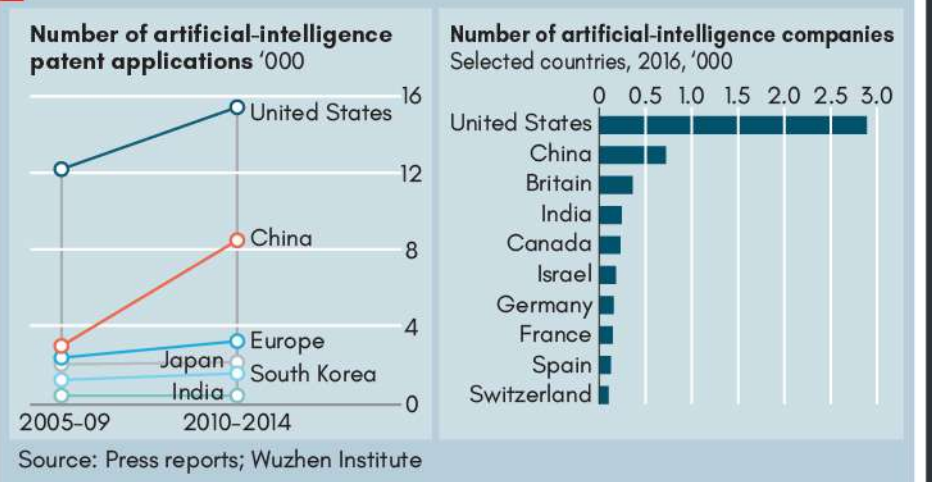
Will AI's penetration into national security affect the global geopolitics?

In 2017, China announced the Next Generation Artificial Intelligence Plan with an aim to assume global leadership in AI innovation.In 2019, Russian President made a statement- "He who can establish a monopoly in artificial intelligence... will rule the world."Recently, US announced the "American AI Initiative" for advancing AI capabilities.

These developments highlight the **importance that AI is assuming globally.** As we move towards the middle of the 21st century, it is becoming clearer how a **nation's strength in AI** is becoming **increasingly intertwined to its geopolitical standing.** In this context, success in AI has the potential to alter the current balance of power between countries. For instance, if there is no clear domination in the domain of AI by any one country, it could **increase multipolarity in the world order.**

Healthy competition among countries can lead to faster and equitable growth of AI. But, if this **competition intensifies it could take some ugly turns:**

RACE OF THE MACHINE



Source: Press reports; Wuzhen Institute

- **Potential for a new Arms Race:** Proliferation of AI in weapon systems in combination with absence of international regulation on their development could lead to a new trilateral Arms race between US, China and Russia. For example, **Russia's Kalashnikov** (creators of AK-47) is **integrating neural nets with big guns** creating an AI enabled warfare technology.

- Also, China has publicly stated that they want to "**increase government spending on core AI programs** to $22 billion in the next few years, with plans to spend nearly $60 billion per year by 2025".

- **Create trust deficit:** AI based tools create a potential to wage continuous asymmetric warfare. For example, there have been allegations that Russia interfered in 2016 US presidential elections. Such a scenario will create **global trust deficit and make global cooperation extremely difficult.**
  - **Discourse in Russia over theories like 'Gerasimov Doctrine'** indicate that the developments in this direction have already started happening. (Gerasimov doctrine aims at combining military, technological, information, diplomatic, economic, cultural and other tactics for the purpose of achieving strategic goals.)
- **Questions on National Sovereignty:** The dual-use nature of AI based tools creates a scenario where **non-state actors (especially technology giants like Google, Facebook etc.)** also hold significant resources (both technological and human) and thus have the potential for weaponization of AI. This **limits the control that the national governments and global institutions** have over security. For example-
  - **Swarms of bots, Facebook dark posts and fake news** websites have claimed online territory.
  - In **China,** tech giants Alibaba and Tencent have deployed **millions of cameras equipped with facial recognition** to commodify continuous streams of intimate data about citizens.
  - In **Myanmar,** a UN report confirmed that Facebook posts have fueled virulent hate speech directed at Rohingya Muslims **through their psychological profiling using AI.**

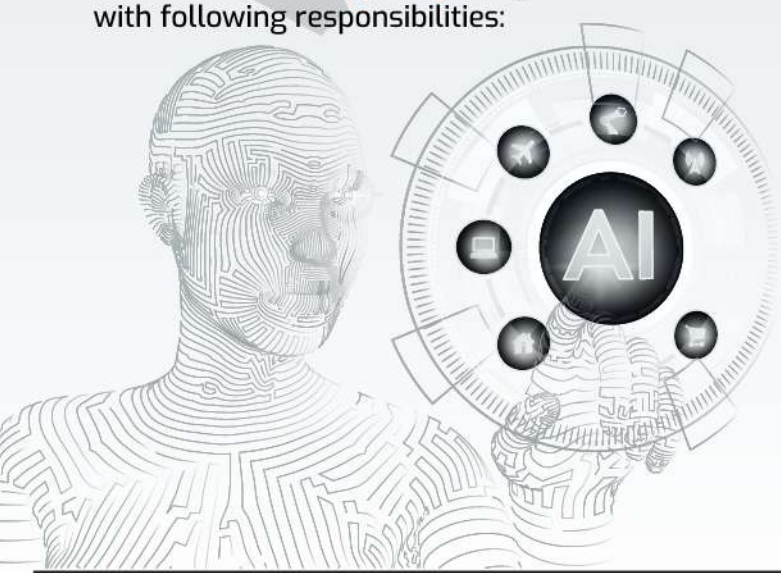
But development of AI **need not be a Zero-sum game.** Collective development of AI in National Security could help us **combat the global security threats like terrorism, smuggling, piracy, trafficking etc.** To enable this collective growth, the Centre for Policy Research at the **United Nations University has created an "AI and Global Governance Platform".** It will act as an inclusive space for researchers, policy actors, corporate and thought leaders to **explore the global policy challenges raised by artificial intelligence.** Apart from this, other efforts that have been made include OECD principles on AI and European Union Communication document and Ethics document on AI.

What are the steps taken by India to tap this opportunity?

In 2018, government constituted a **task force under Natarajan Chandrasekharan** comprising representatives from the government, services, academia, industry, professionals and start-ups to prepare a road map for Artificial Intelligence for national security purposes.

The Government accepted majority of its recommendations in 2019, thus creating an **institutional framework for adoption of AI in National Security.** Following can be cited as key facets of this framework:

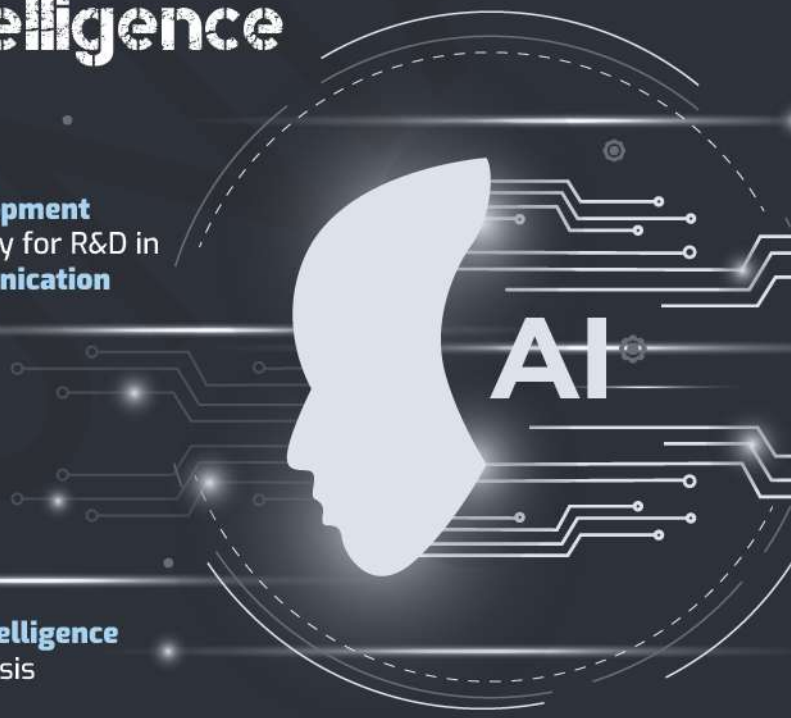
- **Defense AI Council (DAIC):** A high-level DAIC has been created under the chairmanship of Defense Minister with following responsibilities:



- Provide **strategic direction towards AI driven transformation** in Defense.
- Provide guidance and **addressing issues related to data sharing.**
- Provide guidance in building **strategic partnership with industry.**
- Review recommendations concerning **acquisition of technology and startups.**
- Review the **ethical, safe, secure and privacy** assured usage of AI in defense.
- Set policies in partnership with government institutions and industries to **create deterrent for social and technology misuse.**

- **Defense AI Project Agency (DAIPA):** It also envisages to establish a DAIPA with Secretary (Defense Production) as its ex-officio Chairman. The key responsibilities of DAIPA will be to-
  - Evolve and adopt a **preferred technology stack within Defense establishments** for development of AI Use Cases.
  - Evolve and **adopt standards for technology development** and delivery process for AI projects.
  - Formulate policy for **Intellectual Property Rights (IPR).**
  - **Enable and review** the delivery of AI projects.
  - Incentivize the use of AI in existing systems and processes that demonstrate operating benefits.
  - Formulate policy for selection of, and contractual engagement with **strategic industry partners.**
- **Integration of AI into India's Defense Strategy:** All organizations in Ministry of Defense have been asked to integrate and embed AI, in an appropriate manner, in their strategies. These include the three Services, the Coast Guard, DRDO and DPSUs among others.
- **Capacity Building within Defense** through:
  - **AI training courses** in all defense training centers and institutes.
  - **AI training of defense personnel** in order to develop a critical mass of in-house data analysts, data scientists and AI specialists.

Centre of Artificial Intelligence and Robotics (CAIR)

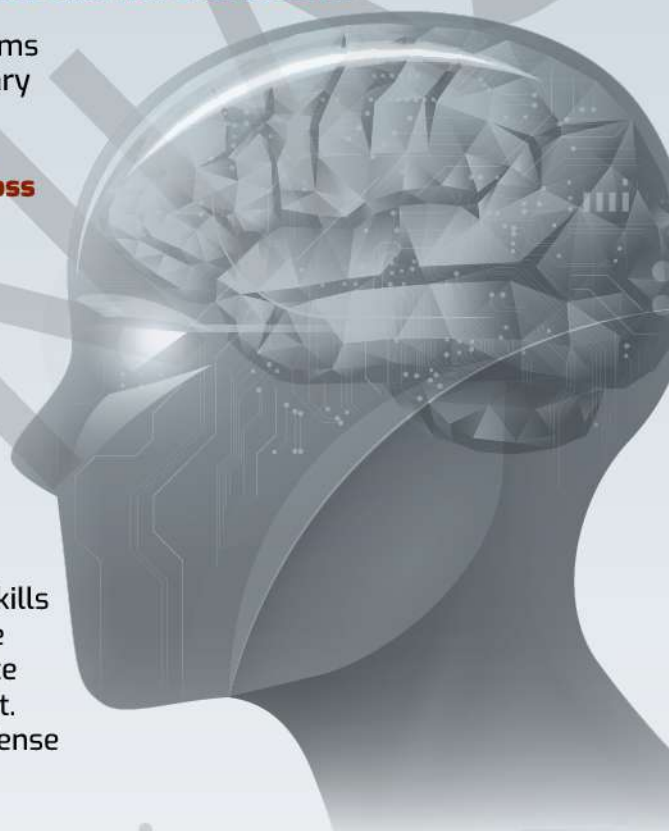


- It is **laboratory of the Defense Research and Development Organization (DRDO).** CAIR is the primary laboratory for R&D in different areas of **Defense Information and Communication Technology (ICT).**
- It has a comprehensive library for AI-based algorithms and data mining toolboxes that can potentially be used for image/video recognition, Natural Language Processing **(NLP),** and swarming (learning from observing nature and applying the concepts to machines).
- Currently, CAIR is developing an **AI-based Signal intelligence solution** to enhance intelligence collation and analysis capabilities of the armed forces.

What are the potential challenges in adoption of AI for National Security?

- **Absence of clarity on 'what is AI' and 'what we intend to do' among policymakers:** There is a limited understanding of key questions like- What kind of AI do we want? Do we require fully autonomous drones to engage with the adversary aircraft in a dogfight or deploy autonomous patrolling vehicles at the borders for getting the job done? How much autonomy should be given to the machines on the battlefield? Etc.
  - A clear vision of the AI Programme is necessary for a middle-income country like India as we **cannot afford to invest heavily** in this sector at the cost of development.
- **Lack of critical infrastructure:** It is one of the biggest impediments in the prospects of AI in India for both civilian and military uses. As AI runs complex algorithms on loads of data, it is essential to have robust hardware and enabling data banks within the country.

- **Development of Ethical Standards:** Use of AI in defense would raise a large number of ethical questions like- Who holds the accountability in case AI does not perform as predicted? How can AI be integrated with current protocols followed in the forces? How far AI can be trusted for the protection of the country? Development of these ethical standards is a prerequisite for adoption of AI for National Security.
- **Increased vulnerability to cyberattacks:** The proliferation of AI systems will increase the number of "hack-able things," including systems that carry kinetic energy (e.g., moving vehicles), which **may in turn allow exploitive actions to induce lethal effects.**
  - It can also lead to increased instances of crimes like **cyber-espionage,** data theft and proliferation of ransomwares like WannaCry.
  - Also, ensuring that **data is available without compromising the privacy of the entities** or individuals would be a challenge.
- **Theft vulnerability:** AI systems are particularly vulnerable to theft by virtue of being almost entirely software based. For example, a large number of AI tools that have been made for civilian use have been shared widely on unclassified internet sites. Some of these tools can be adapted for use as weapon systems thus making them **accessible to major military powers and non-state actors.**
- **Technology cannot be completely controlled:** Using AI systems can significantly increase the scale and speed at which military operations are conducted. If the pace of operations exceeds human ability to understand and control events, that could **increase a system's destructive potential in the event of a loss of system control.** Also, it has some internal weaknesses:
  - AI systems **can fail in unexpected ways,** for example image processing results in certain cases are extremely poor, thus making them unreliable.
  - AI systems may be **subject to algorithmic bias** as a result of their training data.
  - **"Domain adaptability,"** or the ability of AI systems to adjust between two disparate environments, may also present challenges for militaries.
- **Limited role of private sector in defense:** AI demands high-skills and capital as innovations need an ecosystem supporting the free flow of both money and skill. Thus, the role of the private sector will be pivotal in making the AI accessible and efficient. However, as of now the **participation of private sector** in defense is **both limited and peripheral.**



What can be done to overcome these challenges?

- **Vision document on AI:** India should envisage a clear strategic vision regarding the AI. Having a Vision document provides clarity to policymakers as well as the defense establishments regarding capabilities and envisaged outcomes.

- India is home to **world class academicians** in computer science and engineering spread across the Indian Institutes of Technology **(IITs)**, Indian Institute of Science **(IISc)**, National Institute of Technology **(NITs)** and Indian Institutes of Science Education and Research **(IISERs)**. An **academia-industry-policy synergy** is of utmost importance to realize the strategic, societal and cultural implications of AI in defense.

- **Creation of a supportive ecosystem:**Along with a clear policy, there is a dire need to **invest in critical infrastructure** so that the data servers lie within the territory. Apart from ensuring strategic independence, it will also address data privacy concerns.
- **International cooperation:** To ensure that India is at par with other countries with regard to adoption of AI in National Security, various efforts like joint development, technology sharing, **encouraging development of global policy and standardization** could be done.
  - For instance, India and Japan have finalized the text on cybersecurity agreement that will promote cooperation in key areas such as 5G network and Artificial Intelligence.
- **Tapping the civilian innovation ecosystem:** The AI-market for civilian purposes in the country is on the rise. For instance, India ranks third in G20 countries in AI-based startups. Policymakers could tap this potential for the defense sector. For example, marrying the flagships initiatives of the current government — Make in India in Defense and Digital India — to bring a technological revolution in the defense industry.
- **Balancing adoption and innovation:** Since India is a late entrant in the field vis-à-vis powers like China and US, it could capitalize on the late-movers advantage, i.e., **mimicking the existing narrow-AI technologies,** to fulfil its basic security needs (like border patrols and intel-gathering) alongside **innovating over and above the existing technologies.**

Conclusion

Entry of Artificial Intelligence in the Security domain has showed us the glimpses of the complexity and the need for preparedness that is required to assimilate it. With further growth of AI, the threats it presents and opportunities it creates for national security will progressively multiply.

In the light of this, the nation states and global institutions can see AI as a tool of weaponization creating another cold war like era. Or, it can be adopted in a collaborative global manner which does not disturb already fragile global trust. Whatever be the case, this is the time for India to step up to keep pace with the ongoing technological revolution in the defence arena.

TOPIC AT A GLANCE

Relevance of AI in National Security

- **Changing nature of security:** The traditional elements of security are rapidly expanding with technological developments leading to creation of newer challenges like Hybrid Warfare and Cybersecurity.
- **Higher accessibility of AI based tools** due to their dual-use nature and absence of global regulation.
- **Unavoidable presence of AI** when used in tandem with other technologies. For example, use of AI in Social Media.

Relevance of AI in National Security

Potential Opportunities created

- **Increasing real-time intelligence** with the availability of large data sets for analysis.
- **Creating autonomous and semi-autonomous systems** to increase the reach of military operations.
- **Increased logistical abilities** especially in border areas.
- Advancing **military cyber operations** both in offensive and defensive capacity.
- **Replacing humans in 'dull, dangerous or dirty' work,** thus freeing them up for more complex and cognitively demanding work.

AI, National Security and global geopolitics

- **Major powers** including Russia, USA and China **have taken initiatives** to enhance their capabilities in AI.
- A nation's **strength in AI** is becoming increasingly **intertwined to its geopolitical standing.**
- Potential issues in this scenario-
  - **New Arms Race** due to proliferation of AI in weapon systems.
  - **Creation of global trust deficit** which may hinder global cooperation.
  - **Effect on National Sovereignty** as non-state actors also hold AI resources.
- But AI can also **help combat global security threats** like terrorism, smuggling, piracy etc.
- To enable collective action, several global efforts have been made including United Nations University's "AI and Global Governance Platform".

Potential Challenges

- **Absence of clarity** on 'what is AI' and 'what we intend to do' **among policymakers.**
- **Lack of critical infrastructure** like data banks.
- **Ethical standards** for usage have not been developed.
- Adoption can **increase vulnerability of systems to cyberattacks.**
- **Higher theft vulnerability** due to **software-based** nature of AI systems.
- **Technology cannot be completely controlled or held accountable.**
- **Limited role of private sector** in defense ecosystem leading to lower investments and technology infusion.

Steps taken by India

- The Government has created an **institutional framework for adoption of AI in National Security-**
  - **Defense AI Council (DAIC):** A high-level DAIC has been created to provide for transformation in defense, addressing data sharing issues, partnership with industry and ensure ethical, safe and secure usage among others.
  - **Defense AI Project Agency (DAIPA):** The key responsibilities of DAIPA will be to evolve and adopt suitable technologies, appropriate standards, and IPR policy and review delivery of projects.
- **Integration of AI into India's Defense Strategy:** All organizations in Ministry of Defense have been asked to integrate and embed AI, in an appropriate manner, in their strategies.
- **Capacity Building within Defense** through AI training courses **in order to develop a critical mass of in-house data analysts, data scientists and AI specialists.**
- Other efforts are also being made like DRDO's **Centre of Artificial Intelligence and Robotics (CAIR).**

What more can be done?

- India should envisage a **clear strategic vision regarding AI** taking into account **the strategic, societal and cultural implications of AI in defense.**
- Creation of a **supportive ecosystem** with **increased investment and improved critical infrastructure.**
- **Encourage international cooperation** on the lines of **India- Japan text on cybersecurity.**
- **Tapping the civilian AI- innovation ecosystem** as a large set of these technologies have a dual-use nature.
- **Balancing adoption and innovation:** Since India is a late entrant in the field vis-à-vis powers like China and US, it could capitalize on the late-movers advantage alongside developing its own technological base over and above it.