

# **ARTIFICIAL INTELLIGENCE IN ARMED FORCES- AN ANALYSIS**

**By**

**Maj Gen PK Mallick VSM, (Retd)**

## **Introduction**

Today is the age of the Fourth Industrial Revolution. The current period of rapid, simultaneous and systemic transformations driven by advances in science is reshaping industries, blurring geographical boundaries, challenging existing regulatory frameworks and even redefining what it means to be human. Artificial intelligence (AI) is the software engine that drives the Fourth Industrial Revolution. AI is creating targeted marketing, safer travel through self-driving cars, smarter weapons and new efficiencies in manufacturing processes, supply chain management and agricultural production. It holds the promise of solving some of the most pressing issues facing society, but also presents challenges such as inscrutable “black box” algorithms, unethical use of data and potential job displacement.

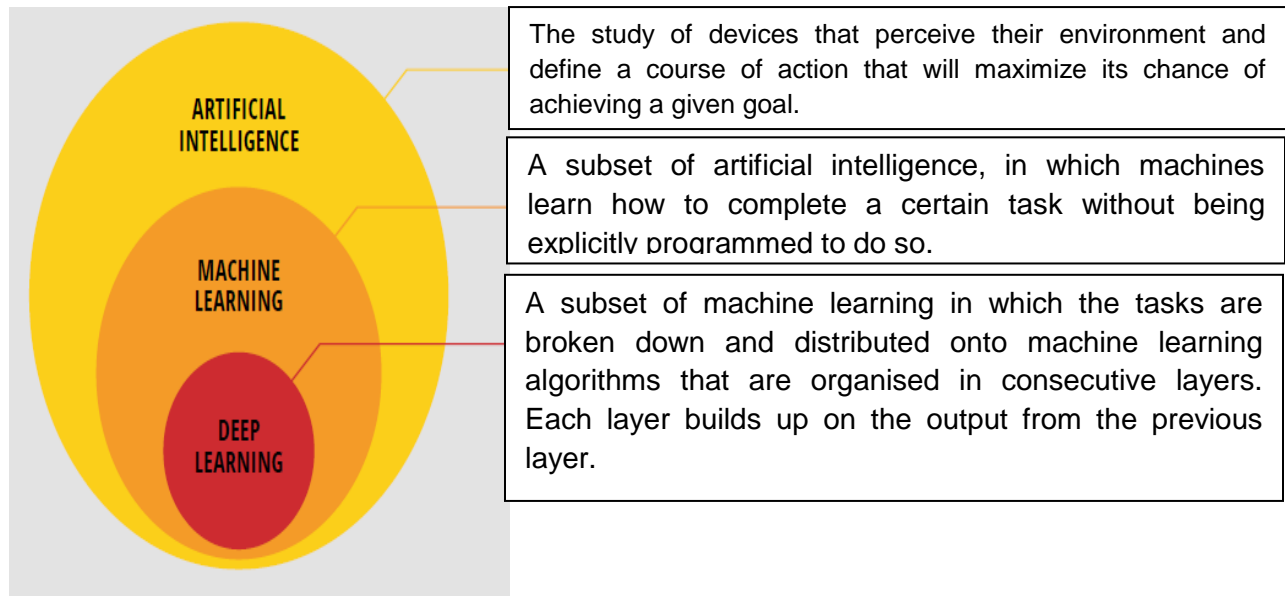
Artificial Intelligence are machine programs that can teach themselves by harnessing High Power Computing(HPC) and big data and eventually mimic how the human brain thinks, supports and enables nearly every sector of the modern economy. Corporations and governments are fiercely competing because whoever is the frontrunner in AI research and applications will accrue the highest profits in this fast growing market and gain a military technological edge. AI itself will not manifest just as a weapon. It is an enabler that can support a broad spectrum of technologies.<sup>1</sup>

These technologies are starting to have a transformative effect on defence capability. AI will have digital, physical and political security implications, expanding existing threats, introducing new threats and changing the character of threats and of war. These changes could include the automation of social engineering attacks, vulnerability discovery, influence campaigns, terrorist repurposing of commercial AI systems, increased scale of attacks, and manipulation of information availability.

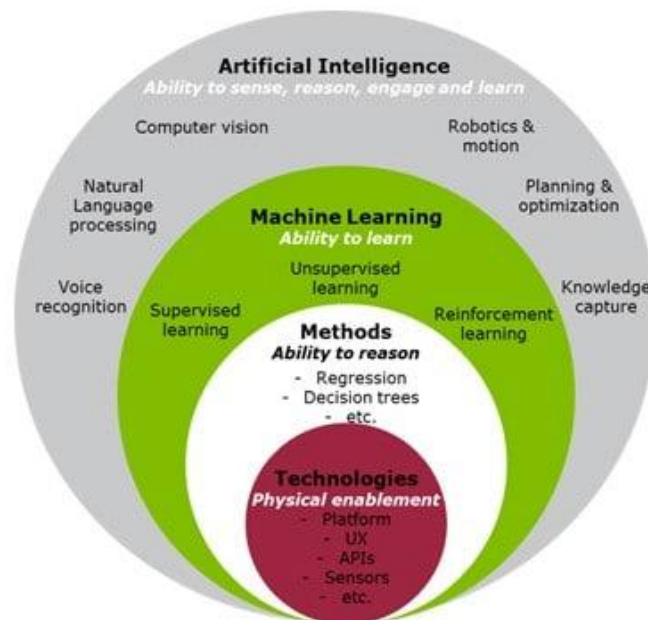
---

<sup>1</sup> Manju Bansal, “AI Is the New Black,” MIT Technology Review, February 27,2017

## Selected AI Definitions



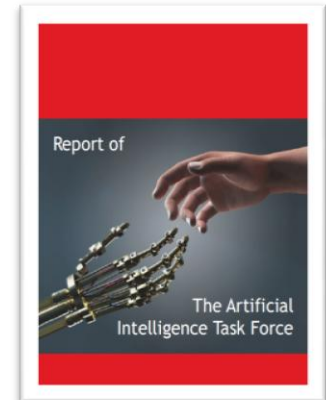
## Different Areas of AI



## National Security

In August 2017, India's Commerce Ministry convened the Task Force on AI for India's Economic Transformation. The Task Force report states :

AI can be a force-multiplier for several national security missions. Potential applications include Autonomous Underwater Vehicles (AUVs) and Unmanned Combat Aerial Vehicles (UCAVs) for underwater and aerial defence operations as well as coastal and border surveillance; robot mules for unburdening soldiers; robots for counter-IED and counter-terrorism operations and close-in-protection systems against cruise missiles and similar aerial threats. In the Indian context, AI can be particularly relevant in securing public and critical infrastructure, especially urban centers, against terrorism by predicting terror attacks; tracking terror financing and recruitment; and monitoring cross-border infiltration. AI techniques can also contribute to strengthening cyber security. The application of AI to national security missions requires new ways for government and public sector institutions to work with industry and academia as well as new ways to incentivize young researchers to participate in national security projects. The use of AI for national security would also require India's active participation in shaping international discussions on regulatory aspects, including ensuring respect for applicable international law and the protection of personal data.



National security imperatives require that technology based force multipliers be developed. Some areas where AI based systems could be usefully deployed include:

- Autonomous surveillance and combat systems.
- Adaptive communications systems.
- AI based cyber-attack mitigation and counter-attack systems.
- Multi-sensor data fusion based decision making systems.

## AI in Armed Forces

Former US Deputy Secretary of Defense Robert O. Work said, "Rapid advances in artificial intelligence and the vastly improved autonomous systems and operations they will enable are pointing towards new and more novel warfighting applications involving human-machine collaboration and combat teaming." The role of educated humans will

begin to concentrate on the higher cognitive tasks of processes such as mission analysis, operational planning, and assessments.<sup>2</sup>

The race to develop and apply meaningful and break through AI is already at full swing and the prize for finishing first is significant. The tech industry giants are investing tens of billions of dollars in their own AI research and development, and venture capitalists are funding an equal amount for new startup companies. Just as industrialization and mechanization changed the fundamental character of both civilization and warfare, and they gave an overwhelming advantage to the side that was first, break through AI could have an exponentially greater effect.

AI and human computer interfaces offers the Armed Forces opportunities for leap ahead offset over potential competitors. In the future, individuals, teams, units and the entire force could operate far more cognitively connected than today. There is great potential for common understanding, collective decision making and unified anticipatory action. In future conflict, ambiguity will increase despite interconnectedness. The velocity and scale of activity will make it difficult to discern the important from the unimportant and what is real from what is fake. Adversary spoofing, deception and data manipulation and corruption will create a common operational picture that is part fact, part fiction. This murky situational awareness will feed decision cycles that will be compressed by pervasive data and near instantaneous communications.

Artificial intelligence can operate in several dimensions like :

- It can be used to direct physical objects, such as robotic systems, to act without human supervision. Whether in tanks, planes or ships, AI can help reduce the need to use humans, even remotely, or as part of human machine teams. Swarm techniques, generally involve the creation of supervised algorithms that direct platforms such as drones.
- AI can assist in processing and interpreting information. Image recognition algorithms can be used for tagging. Project Maven is a U.S. military program that seeks to develop algorithms to automate the process of analyzing video feeds captured by drones.
- Overlapping narrow AI systems could be used for new forms of command and control, operational systems including battle management, that analyze large sets of data and make forecasts to direct human action or action by algorithms.

---

<sup>2</sup> Robert O. Work and Shawn Brimley, 20YY: *Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014).

- Future AI systems offer the potential to continue maximizing the advantages of information superiority, while overcoming limits in human cognitive abilities. AI systems, with their near endless and faultless memory, lack of emotional investment and potentially unbiased analyses, may continue to complement future military leaders with competitive cognitive advantages.

By distancing the human from conflict, the technology lowers not only the costs and risks associated with war, but the political bar to initiating hostilities as well. Legacy attributes of the Army such as flexibility, mobility and expeditionary skills may be replaced by new attributes such as predictive, continuously learning, unknowable, decentralized and compelling. This new set of attributes will be enabled by AI technology capabilities. These technologies have the potential to change the character of conflict.

**The Nature and Character of War.** Military professionals swear by the Maxim by the Prussian Clausewitz : war's nature does not change—only its character. The former describes what war is and the latter describes how it is actually fought. War's nature is violent, interactive and fundamentally political. The *character* of war describes the changing way that war as a phenomenon manifests in the real world. War's conduct is undoubtedly influenced by technology, law, ethics, culture, methods of social, political, and military organization and other factors that change across time and place. The character of warfare changes in concert with the tools that become available and how they influence the ways militaries organize themselves to fight wars.<sup>3</sup>

There is an argument that AI has the potential to go beyond shaping the character of war and change the nature of war itself. AI could alter the nature of war itself because wars will be fought by robotic systems, not people. AI has the potential to engage in planning and decision making that were previously human endeavours. U.S. Defense Secretary James Mattis speculated in February 2018 that AI is “fundamentally different” in ways that raise questions about the nature of war. The character of warfare will clearly change, and these changes could significantly influence the Clausewitzian elements that frame our understanding of war's nature.

---

<sup>3</sup>*From a Clausewitzian perspective, that war is human fundamentally defines its nature. Carl von Clausewitz, On War, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989).*

Autonomy will change the nature of war in several ways. These are<sup>4</sup> :

- It could weaken the role of political direction by forcing response delegation to lower echelons for faster forms of attack.
- Autonomy can lessen the ability of governments to gain the support and legitimacy of their populations, while making it easier for foreign governments to manipulate their adversary's populations.
- Deep learning forms of AI will augment the intuition and judgment of experienced commanders.
- Automated technologies could reduce popular support for professional military institutions, which paradoxically could free governments to employ force more readily since the political consequences are reduced.
- As with the earlier ages, friction and uncertainty will endure.
- The age of autonomy can introduce new forms of friction while reducing human factors in tactical contexts.

The most significant elements of war, violence, human factors, and chance, will certainly remain. So, too, will fog and friction. War's essence as politically directed violence will remain its most enduring aspect, even if more machines are involved at every level. As technology advances at rapid pace the nature and character of war will be changed. In the upcoming military revolution of autonomy, we will have to consider new sources of combat power and assess how they impact each level of war.<sup>5</sup>

## **US DoD Strategy**

DoD of USA has developed a multi decade strategy for applying a suite of advanced technologies to nearly every facet of its operations. In the first phase, the DoD will create a more intelligent force, using AI to enhance platforms, munitions and decision processes. As these technologies mature, the DoD aims to create a more autonomous force, pairing AI enabled systems with human military personnel to accentuate the strengths of each, enabling faster decisions and better combat outcomes. In the more distant future, "swarms" of advanced cognitive robots may redefine combat operations in the battle space. This is explained in the following diagram as Exhibit 1.

---

<sup>4</sup> Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," Journal of Strategic Studies 39, no. 5-6(2016): 793-819, <https://doi.org/10.1080/01402390.2015.1088838>

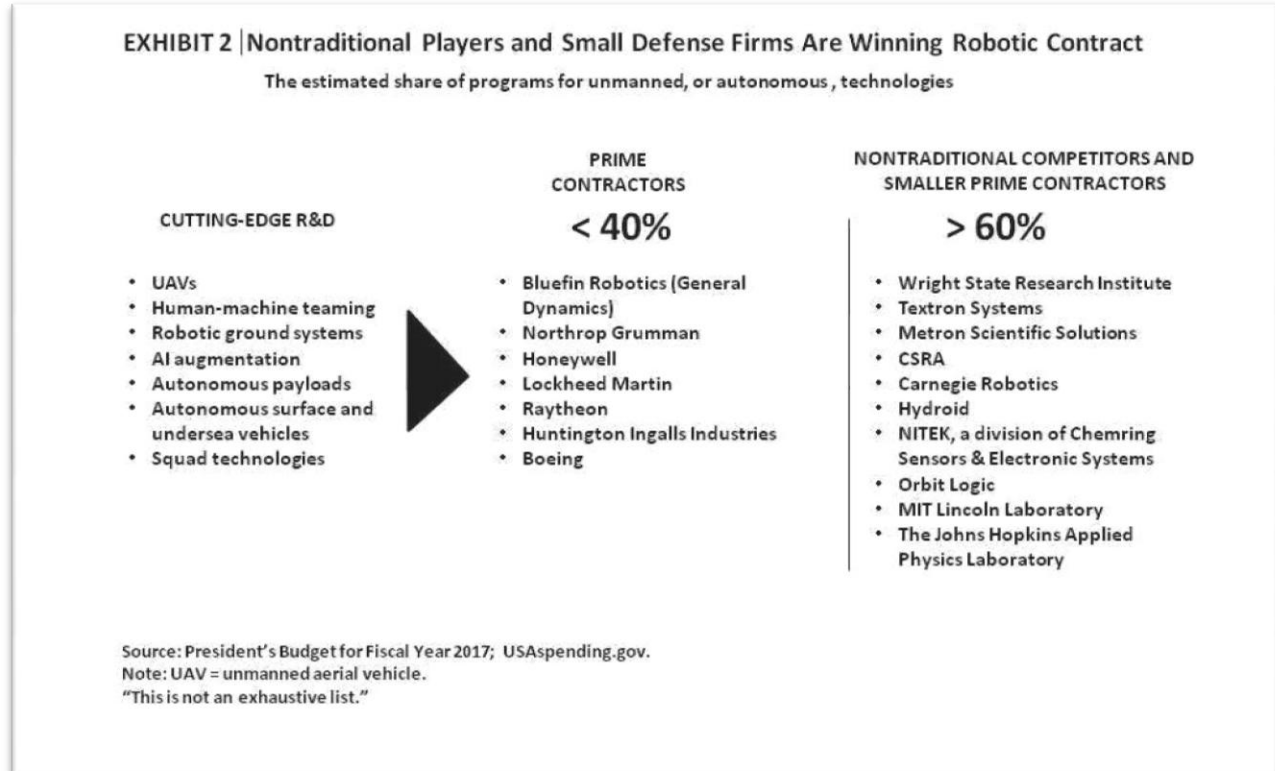
<sup>5</sup> F. G. Hoffman, Will War's Nature Change in the Seventh Military Revolution?, Parameters 47(4) Winter 2017–18, [https://ssi.armywarcollege.edu/pubs/parameters/issues/Winter\\_2017-18/5\\_Hoffman.pdf](https://ssi.armywarcollege.edu/pubs/parameters/issues/Winter_2017-18/5_Hoffman.pdf)

### EXHIBIT 1 | AI and Robotic Will Affect Virtually Every Aspect of US Military Operation

		LAND	SEA	AIR	SPACE	CYBER
US battle network	Sensors	<ul style="list-style-type: none"> <li>Sensor-laden Robotic ground vehicles</li> </ul>	<ul style="list-style-type: none"> <li>Long-endurance Autonomous surveillance</li> </ul>	<ul style="list-style-type: none"> <li>Sensing distributed to "attributable," or unmanned, wingmen</li> </ul>	<ul style="list-style-type: none"> <li>AI- enhanced situational awareness in space</li> </ul>	<ul style="list-style-type: none"> <li>AI- enabled cyber-monitoring and triage</li> </ul>
	Command, control, Communications, and intelligence	<ul style="list-style-type: none"> <li>Autonomous AI processing</li> <li>Cooperative human-machine interfaces and augmented decision making</li> </ul>				
	Effects	<ul style="list-style-type: none"> <li>Armed ground vehicles</li> <li>Intelligent nonkinetic engagement</li> </ul>	<ul style="list-style-type: none"> <li>Autonomous "swarms" of small robotic platforms</li> <li>Systems to counter UAVs, surface swarms</li> </ul>	<ul style="list-style-type: none"> <li>Attributable wingmen capable of conducting air-to-air combat</li> </ul>	<ul style="list-style-type: none"> <li>Autonomous antisatellite counter-measures</li> </ul>	<ul style="list-style-type: none"> <li>AI- enabled cyber offense and cyberdefense</li> </ul>
	Logistics	<ul style="list-style-type: none"> <li>Autonomous support (for example, pack robots, resupply systems, and aerial refueling UAVs)</li> <li>Modernized distribution centers optimized with warehouse robots, industrial Internet of Things, and big data</li> </ul>				
Force delivery (for example, training)		<ul style="list-style-type: none"> <li>Physical or virtual autonomous systems for use in training</li> <li>Greater demand for simulation equipment and service</li> </ul>				

Source: Robert o. Work and Shawn Brimley, 20YY: Preparing for war in the Robotic Age, Center for a New American Security , January 22,2014; BCG analysis.  
Note: UAV = unmanned aerial vehicle.

The DoD is bringing in key technologies from commercial industry, increasing the scope of competition that prime contractors face. Prime contractors may be tempted to cede the AI and robotics market to small niche players or subcontractors. More than 60% of the robotics focused contracts in the President's Budget for Fiscal Year 2017 were awarded to nontraditional defense players or small prime contractors as shown in the following diagram Exhibit 2



## Trends

The following trends have emerged<sup>6</sup> :

**The Military Exploitation of Artificial Intelligence (AI) and Autonomous Systems Is Inevitable.** The challenges and realities of big data, complex networks and systems, uncertain environments, ubiquitous and intense peer competition are drivers in both the commercial and military spaces and steer each toward a common set of solutions. Once advanced AI is achieved, it will quickly spiral into almost every area of the commercial, governmental and military domains.

**Early Adoption of AI enabled technology Is Critical Because Potential Adversaries Will Develop and Field Capabilities without Constraint.** These leap ahead capabilities could be so game changing that the difference between finishing first and finishing next could mean years of decisive advantage in every meaningful area of warfare. The legacy combat systems, even with version improvements and upgrades,

<sup>6</sup> US Army Training and Doctrine Command (TRADOC), The Operational Environment and the Changing Character of Future Warfare (Fort Eustis, VA: 2017),



may well be rendered outmatched and ineffective by AI-enabled unmanned autonomous systems, cyber dominance and swarms.

**Significant Acquisition, Budget, and Cultural Inertia Exists Which Could Impact the Army's Ability to Gain Advantages with AI Technologies.** The Armed Forces currently takes a risk adverse approach to acquisition and requirements, waiting for technologies to mature before prototyping and experimentation. In order for the armed forces to become an innovative organization, it must promote an innovative culture, accept risk and leverage new ideas, while collaborating and partnering on experiments to enhance creativity.

**Leader Development for a AI Technologies Must Begin Now.** The current Army Leadership Requirements Model addresses leader development focused on human to human relationships, but the future will challenge leaders with more human machine relationships.

**The Moral Considerations of AI Technologies Should be Addressed Before the Technology Matures.** AI Technologies increasingly remove the soldier from the conflict. The Army must begin to mitigate the potential harmful impacts of these technologies now. Operators of unmanned and semi autonomous systems must understand how the AI processes moral dilemmas, the potential ethical shortcomings of these decisions and how to ensure ethical decisions are made.

**The AI Technologies May Create Unintended Risks by Lowering Risk Thresholds, Subsidizing Foreign Modernization Efforts, and Increasing the Risk of Nuclear War.**

### **Effect of AI Technology on Warfare**

**Intelligence, Surveillance, and Reconnaissance.** Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) are reaching new heights of efficiency that enable data collection and processing at unprecedented scale and speed. AI is useful in intelligence due to the large data sets available for analysis. AI automates the work of human analysts who currently spend hours sifting through videos for actionable information. The human analysts have more time to make efficient and timely decisions based on the data.

**Military drones for surveillance.** Military units across the world are employing drones to:

- Channel remote communication, both video and audio, to ground troops and to military bases.
- Track enemy movement and conduct reconnaissance in unknown areas of a war zone.
- Assist with mitigation procedures after a war by searching for lost or injured soldiers and giving recovery insights for a terrain.
- Aid with operations like peace keeping and border surveillance.

While drones help in guarding aerial zones, robots can be deployed on land to assist soldiers in ground operations. Robot fleets function like soldier units and carry out collaborated armed activities using multiple techniques. They are self reliant, adaptable, and have their fault tolerant systems, all of which contribute to their ability to make and execute decisions swiftly and competently.

**AI Assisted Decision Making.** AI assisted decision making could help leaders at all levels rapidly design, plan and evaluate operations. Through a continuous deliberative planning process, the AI could update and evaluate the plans against the operational environment. The AI would continuously monitor the environment and warn planners when assumptions are no longer valid or if there is an opportunity to improve the plans. The true power of AI will be in the teaming of the human mind with the AI mind. This type of man machine teaming will combine human strengths of goal setting, creativity, and ethical thinking with AI strengths of rational thought through self-taught experience, intuition and deep forecasting.

**Ai Assisted Common Operating Picture (COP).** It would catalog and display a disposition of friendly and enemy forces, automatically built and updated through a big data approach. Despite incomplete intelligence, an AI supported COP could tell where an enemy should be with a corresponding level of confidence. In real time, the AI would continuously interpret the situation, explore multiple lines of effort and determine which is most likely to meet the given success criteria. Based on this, the COP would recommend next actions and predict likely enemy responses.<sup>7</sup>

**Cyberspace.** AI systems play a powerful role in cyberspace for both defensive and offensive measures. AI systems can perform predictive analytics to anticipate cyber attacks by generating dynamic threat models from available data sources that are voluminous, ever-changing and often incomplete. These data include the topology and

---

<sup>7</sup> Sean Kimmons, "With multi-domain concept, Army aims for 'windows of superiority'," U.S. Army, November 14, 2016, available at [:https://www.army.mil/article/178137/with\\_multi\\_domain\\_concept\\_army\\_aims\\_for\\_windows\\_of\\_superiority](https://www.army.mil/article/178137/with_multi_domain_concept_army_aims_for_windows_of_superiority)

state of network nodes, links, equipment, architecture, protocols and networks. AI may be the most effective approach to interpreting these data, proactively identifying vulnerabilities and taking action to prevent or mitigate future attacks.

**Logistics.** AI is expected to play a crucial role in military logistics and transport. The effective transportation of goods, ammunition, armaments, and troops is an essential component of successful military operations. AI has the potential to help the larger Army reshape its tooth to tail ratio and free up additional soldiers for critical areas like combat arms and intelligence, surveillance and reconnaissance.

## **Intelligence**

The Intelligence Community(IC) faces daunting challenges of volume and velocity as well as an ever increasing complexity of variety of data. The IC is challenged to acquire, manage, correlate, fuse, and analyze ever increasing amounts of data across agencies. Data in the IC are generated in too many diverse formats, in too many disconnected or inaccessible systems, without standardized structures and without overarching agreed upon ontology. This situation risks wasted collections, lack of timeliness, missed indications and warnings and lack of relevance for decision making. The result is an inability to fuse data to create multi sourced intelligence as early in the intelligence cycle and as close to the point of collection as possible. Analysts are given a task too difficult, too cumbersome and with too many hurdles to clear to provide timely and relevant analytic judgments or actionable intelligence to policymakers and warfighters.

Artificial intelligence and machine learning will be instrumental to increasing the effectiveness of the future intelligence analyst workforce, improving the odds of gaining and sustaining a competitive or temporal advantage. Digital transformation, methodic multi domain data integration, and algorithmic warfare will be the heart of the intelligence enterprise's role in sustaining a long-term competitive advantage.<sup>8</sup>

Intelligence challenges should be addressed by:

- Embracing machine-learning algorithms that can parse data, learn from the data, and then respond.
- Encouraging creativity and deep thinking by intelligence professionals.

Designing the policy, information technology (IT), agile acquisition, and security environment that allows human-machine tradecraft to flourish.

---

<sup>8</sup> Cortney Weinbaum and John N.T. Shanahan, Intelligence in a Data-Driven Age, Joint Force Quarterly 90, July 3, 2018.

The following actions need to be taken :

- Intelligence analysts need to be trained on how to recognize attempts by an adversary to use altered or manipulated data, including understanding how to use AI to maximum advantage to prevent even the more sophisticated influence operations from affecting desired operational outcomes.
- Data should not be treated as an IT problem; instead, IT systems should be framed by the operational problems they solve. Rapid data access requires effective data management, which calls for new skill sets and expertise, such as data architects and data scientists. Network access across all security domains, access to all relevant data types and agile integration of disruptive technologies are key to achieving and sustaining decision advantage.
- Publicly available information and open source information will provide the first layer of the foundation of our intelligence knowledge.

More emphasis needs to be given to analysts that have to sift through and make sense of the huge data. How has their training changed to account for a more technologically advanced battlespace? How have their products and solutions integrated requirements and workflows with real time information to truly augment their efforts?

**Autonomous Weapons Systems (AWS).** Autonomous weapons systems (AWS) offer potential advantages in future warfare but also present many legal and ethical challenges in addition to the inherent risk in turning over decision making to machines. Question arises if an AWS engages and kills civilians, then who is responsible? What role does the military perform in making ethical decisions if machines and algorithms are executing them?

### **Drones.**

When two drones, each equipped with a kilogram of powerful plastic explosives, were used on August 4, 2018 to attempt to assassinate Venezuelan President Nicolas Maduro, it may have ushered in a foreboding new era—terrorism by unmanned aircraft. That the drones were able to get so close to a world leader at a public outdoor event in Caracas, Venezuela, speaks to how easy drones are to use and how difficult they are to defend against. The use of weaponized drones by lone individuals and small groups, some acting as proxies of nation states, is no longer just a concern for the future, but very much for the present.

Lone actors or small cells of terrorists, criminals, or insurgents can effectively harness the tactical flexibility of a small drone to wreak havoc, including potentially using a drone to take down an airliner. State sponsorship of terrorist groups also increases the likelihood of drone attacks, since states can provide the necessary equipment and training, ensuring that terrorist attacks featuring weaponized drones is a near fait accompli in the not so distant future.

Since so many countries are now using armed drones in combat, Nigeria, Pakistan, and Turkey have recently done so, the chances for sophisticated drone technology getting into the wrong hands increases exponentially. If a terrorist group can steal or purchase a drone from a rogue state or corrupt military or intelligence officials, then they could rely on the myriad online videos posted that essentially demonstrate how these unmanned systems could be used to conduct an attack.

One nightmare scenario universally feared by law enforcement and security services is the use of a small drone to deliver chemical or biological agents in an attack. The possibility that drones could be used to disperse deadly agents or viruses over a sports stadium or public gathering place is a harrowing prospect.<sup>9</sup>

**AI and Degradation of Truth.** Sophisticated AI programmes can now manipulate sounds, images and videos, creating impersonations that are often impossible to distinguish from the original. Deep learning algorithms can, with surprising accuracy, read human lips, synthesize speech and to some extent simulate facial expressions. On the eve of an election, Deepfake videos could falsely portray public officials being involved in money laundering; public panic could be sowed by videos warning of non-existent epidemics or cyber attacks; and forged incidents could potentially lead to international escalation.

**Swarm.** The Armed Forces should adopt a “swarm mindset.” This change would largely be seen in the movement away from the single, exquisite weapons platforms to those that are small, cheap, unmanned, expendable and fast. There are many operational advantages of swarms in terms of autonomy, quantity and speed. Unmanned systems can take greater risk by reducing survivability while maintaining lethality and increasing deployability.

---

<sup>9</sup> Colin P. Clarke, *Drone terrorism is now a reality, and we need a plan to counter the threat*, 20 Aug 2018, available at: <https://www.weforum.org/agenda/2018/08/drone-terrorism-is-now-a-reality-and-we-need-a-plan-to-counter-the-threat/>

**Ethical considerations.** The ethical question of whether or not lethal autonomous-weapons systems (LAWS) should be permitted to make life and death decisions is receiving much attention. Several countries continue to develop LAWS that would be capable of completely independent operation if desired. The Vice Chairman of the Joint Chiefs of Staff, US Air Force General Paul Selva, has argued that humans should be kept in the decision making loop. The UK's foreign office did not support an explicit prohibition on the use of LAWS, because it felt international humanitarian law (IHL) provided sufficient regulation. The UK armed forces, however, only operate weapons systems that are subject to human oversight and control.<sup>10</sup>

### **The Impact of AI on the Balance of Power**

Countries around the world are becoming increasingly aware of the potential economic and social benefits of developing and applying AI. There has been tremendous activity concerning AI policy positions and the development of an AI ecosystem in different countries over the last 18 to 24 months. The US published its AI report in December 2016; France published the AI strategy in January 2017 followed by a detailed policy document in March 2018; Japan released a document in March 2017; China published the AI strategy in July 2017 and U.K. released its industrial strategy in November 2017<sup>11</sup>.

Global investments in artificial intelligence for economic and national security purposes are increasingly described as an arms race. China in its AI Strategy proposed a coordinated strategy to “build China’s first mover advantage” and lead the world in AI technology. Russia is investing heavily as well, especially in the military domain. In robotics, Russia is deploying remotely piloted tanks, such as the Uran-9 and Vohar, on the battlefield.

The character of AI technology, like robotics, makes many countries well-positioned to design and deploy it for military purposes. In Southeast Asia, Singapore is on the cutting edge of AI investments (both military and non-military). Other Southeast Asian nations are making advances in AI research as well. In the military domain, South Korea has

---

<sup>10</sup> Peter Maure, *Algorithmic warfare is coming. Humans must retain control*, 26 Sep 2018, <https://www.weforum.org/agenda/2018/09/algorithmic-war-is-coming-humans-must-retain-control/>

<sup>11</sup> Development, Concepts and Doctrine Command, Strategic Trends Programme: Global Strategic Trends—Out to 2045, 5th ed. (Shrivenham, UK: Ministry of Defence, 2016), 67.

developed the SGR-A1, a semi-autonomous weapon system designed to protect the demilitarized zone from attack by North Korea.

## India

"New and emerging technologies like AI and Robotics will perhaps be the most important determinants of defensive and offensive capabilities for any defence force in the future. India, with its leadership in information technology domain, would strive to use this technology tilt to its advantage"

– Prime Minister Narendra Modi

AI Task Force Report by Ministry of Commerce and Industry states on National Security:

- Given the multi disciplinary nature of the task, a consortium of MSME industries to be created for development of autonomous systems such as UAVs and UUVs, including subsystems and components.
- Provision of grants, realistic data and cyber security tools to develop methodologies for protecting digital assets and data from external cyber threats and attacks.
- Existing infrastructure including NATGRID, Humanit (Human Intelligence), SIGINT (Signal Intelligence), COMINT (Communication Intelligence), Imagery data and video surveillance from aircrafts, CCTV data from urban areas and critical infrastructure locations, and, Radar data and Satellite Imagery to be integrated on a unified platform. AI based Techniques to be embedded in the backbone of the platform to provide need based real time information to various security agencies involved in threat mitigation.

While there is no official military strategy document on the uses of AI in the battlefield yet, there are several potential applications that, as Shashank Reddy of Carnegie India puts it, are “low-hanging fruit.” Among these applications are logistics and supply chain management, cyber operations, intelligence and reconnaissance.<sup>12</sup>

R&D on defense applications of AI is conducted under the Center for Artificial Intelligence and Robotics (CAIR), established by the Defense Research and

---

<sup>12</sup> R. Shashank Reddy , *How AI can help the Indian Armed Forces*, Mar 05 2018, available at : <https://www.livemint.com/Opinion/EzKziDVFvruJ0KLJF7ySQM/How-AI-can-help-the-Indian-Armed-Forces.html> ,

Development Organization (DRDO) in 1986. In the three decades since, CAIR has worked on building integrated, networked information systems, data mining tools, robotics, and other AI-enabled products for the Indian military.

AI would greatly improve the ability of Indian forces to secure the 8,600 miles of land borders it shares with other countries. For instance, Border Security Force (BSF) is working on a pilot program called the Comprehensive Integrated Border Management System (CIBMS), which would put in a place an electronic surveillance system monitored by BSF personnel. Integrating AI-enabled image recognition and automated alerts into the system would greatly aid in the speed and efficiency of a BSF response.

Another practical application of AI is in improving battlefield operations using all-terrain reconnaissance. In February 2018, the DRDO successfully tested the Rustom 2 UAV, and is reportedly developing a “Multi Agent Robotics Framework” (MARF), a system that will enable the Indian Army’s many battlefield robots to collaborate with each other on surveillance and reconnaissance. The DRDO is also developing Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) UAVs to detect radiation, as well as Remotely Operated Vehicles (ROVs) for surveillance and IED disposal.

To fully exploit their potential, the Indian military needs to build a close working relationship with the vibrant private technology sector in India, and especially with start-ups doing exciting work in the AI space. This will involve handing over potentially sensitive data to private firms so as to enable the building of AI systems that can meet the specific needs of the Indian Armed Forces. This is entirely uncharted territory. To assuage the valid concerns that may arise with sensitive data being in private hands, a unique legal “trust model” needs to be built that accounts for the needs of the military and technological innovation. While the development of such a model may, in fact, prove to be a tougher task than the simple integration of AI technologies, it needs to be done if the Indian military is to prepare itself for warfare in the 21st century.<sup>13</sup>

## Conclusion

Big-data analysis and machine-learning algorithms are already available and vastly expand information processing capabilities. AI is already a military reality. Automated decision-making will play an increased role at every level of the command and control

---

<sup>13</sup> Amber Sinha, Elonnai Hickok and Arindrajit Basu, *AI in India: A Policy Agenda*, *The Centre for Internet and Society*, available at : <https://cis-india.org/internet-governance/blog/ai-in-india-a-policy-agenda>



process, from swarming miniature UAVs to the national command authority. Genuine AI in the scientific sense may still be years away, but it is not too early to begin establishing normative limits for LAWS through IHL and military rules of engagement, in anticipation of this eventuality.<sup>14</sup>

In addition to these battlefield roles, AI will transform other military activities, including logistics, intelligence and surveillance and even weapons design. Collectively, these activities, mostly tactical in nature, will have a transformative effect on the strategy of those states employing them. This is because militaries that can successfully develop and utilise them will experience a dramatic increase in fighting power relative to those that cannot.

At present, many pertinent AI technologies are immature. Modern unmanned aircraft in service can operate autonomously, but cannot yet execute the sorts of complex missions that manned equivalents can achieve. Land robots are clumsy on uneven terrain. Sceptics rightly point to previous bursts of enthusiasm for AI, followed invariably by disappointment and stagnation as concepts fail to deliver significant breakthroughs in autonomous decision making. There is considerable wariness that the hype and publicity surrounding deep learning will not pan out as dramatic breakthroughs. Nevertheless, the rapid progress in AI research, especially of hybrid approaches that utilize multiple AI techniques, along with increasingly powerful hardware on which to run algorithms, suggests the potential for AI to significantly affect existing military activities in the short to medium term, even if it falls short of simulating human level cognition any time soon.

Technological innovations could have large scale consequences for the global balance of power and international conflict. Yet their impact is generally determined by how people and organizations use the technology rather than by the technology itself. Militaries around the world will have to grapple with how to change recruiting and promotion policies to empower soldiers who understand algorithms and coding, as well as potential shifts in force structure to take advantage of AI based coordination on the battlefield. It is too early to tell what the impact of AI will be, but technology development suggests it will have at least some effect.

---

<sup>14</sup> Kenneth Payne, *Artificial Intelligence: A Revolution in Strategic Affairs?*, *Survival: Global Politics and Strategy* October–November 2018. Available at <https://www.iiss.org/publications/survival/2018/survival-global-politics-and-strategy-octobernovember-2018/605-02-payne>