IDSA Occasional Paper No. 49

FUTURE WARFARE AND ARTIFICIAL INTELLIGENCE

THE VISIBLE PATH

ATUL PANT

IDSA Occasional Paper No. 49

Future Warfare and Artificial Intelligence

The Visible Path

Atul Pant

INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-93-82169-80-2

First Published: August 2018

Price: Rs.

Published by: Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
E-mail: contactus@idsa.in
Website: http://www.idsa.in

Cover &
Layout by: Vaijayanti Patankar

Printed at: M/s

Future Warfare and Artificial Intelligence
The Visible Path

Artificial Intelligence (AI) is being viewed as the most disruptive technology of the current era. It is being substantially invested in and intensely worked upon in the scientific and commercial world. It is already showing up for nascent commercial usage in many gadgets and devices like mobiles, computers, web application servers, etc., for search assistance, requirement prediction, data analysis and validation, modelling and simulation, linguistics, psychology, among others. Commercial giants such as Google, Microsoft and Amazon are using AI for consumer behaviour prediction. Since 2011 we have been living in what is being termed as the "cognitive era" because of the increasing infusion of AI in everybody's daily lives.[1] IBM's Watson, which probably was the first AI commercial application for problem solving in varied fields, was launched in 2013. Watson came into the limelight when it defeated the two highest ranked players of all time in the game *Jeopardy* in 2011. Watson has since been improved further.

AI is predicted to pervade into all major civillian systems and gadgets in a major way within a decade or so, forming their software base. Further, in two to three decades, it is predicted that it will totally alter the ways of the

---

[1] Stephan De Spiegeleire, Matthijs Maas and Tim Sweijs, "Artificial Intelligence and the Future of Defence", *The Hague Centre for Strategic Studies*, 2017, available at https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf (accessed 16 March 2018).

world. Major powers like the United States (US), the European Union (EU) and China have already come out with policy documents and roadmaps on development, adoption and promotion of AI in various fields.

Varied definitions have been coined for AI by different experts. All of them converge onto the concept of machines acquiring human-like intelligence, which generally follows a sequence known as the perception–cognition–action (or decision making) information processing loop.[2] AI is programmed to similarly follow the loop, in that the AI computer senses the world around it, and processes the incoming information through optimization and verification algorithms, with a choice of action made in similar ways to that of humans.[3] Various advanced AI capabilities are in various stages of development and usage currently, and include natural language processing, searching information, facial, object or gesture recognition, self-adaptive learning, intuitive perception, comprehensive reasoning, hybrid intelligence (man-machine combined intelligence), collective swarm intelligence, problem solving, prediction and response, among others.[4,5]

The military employment of AI, though a natural derivative of AI development with immense potential and advantages, has been a

---

2 Jeremy Owen Turner, Michael Nixon, Ulysses Bernardet, Steve DiPaola (eds), "Integrating Cognitive Architectures into Virtual Character Design", *Information Science Reference*,Hershey: IGI Global, p. 239.

3 M.L. Cummings, "Artificial Intelligence and the Future of Warfare", "Artificial Intelligence and the Future of Warfare", *Chatham House*, January 2017, p. 3, available at https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf (accessed 14 March 2018).

4 Munish Sharma, "The Global Race for Artificial Intelligence: Weighing Benefits and Risks", *IDSA Issue Brief*, available at https://idsa.in/issuebrief/the-global-race-for-artificial-intelligence_msharma_230218 (accessed 12 March 2018).

5 "New Generation Artificial Intelligence Development Planning Notice No. 35 [2017]", *State Council of China*, issued on 8 July 2017, available at http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm, (accessed 12 March 2018).

contentious issue and a topic often dividing the scientific communities. With the exponentially burgeoning AI and its foray into the military sphere, AI is already reshaping the functioning of militaries in a major way. It will foreseeably radically transform future warfare and military operations. At the same time, warfare itself is undergoing changes at the conceptual level owing to rapid technological advancements. How AI would mould it in future is still being worked out by the pundits. This paper aims to ascertain the proliferation of AI in warfare in the near future—projecting over the next decade or two—in the light of its developmental trajectory and the main issues surrounding its future military use. It also looks for a derivative for India.

The paper begins with a section on the "Classification of AI Systems", wherein the reader will be taken into a slightly deeper understanding of AI, to enable an objective analysis of AI's development and employment trajectory. The section on "Extraordinary Feats" reveals the disruptive nature of the technology. Future growth and proliferation of AI is discussed in the section titled "Future Manifestations". This section also highlights various issues associated with AI, while building on a general understanding of it. The section on "AI Powered Warfare", attempts to derive AI will impregnate the military systems and reshape the warfare including the concepts and doctrines. The paper then focuses on a major issue of "Uncertainty Negotiation" that affects situations where AI is employed; and analyses battlespace employment of AI in that light. The next section analyses the "Challenges" associated with military employment of AI-based systems. The section on "The Global Leadership Race" highlights the global trend in military use of AI, which is followed by an analysis of "India's Position" and some recommendations for Indian policymakers.

Classification of AI Systems

At this point in time the nascent AI that the world is seeing in various gadgets and online software applications are initial forms of what the Defense Advanced Research Projects Agency (DARPA), US calls the first and second wave of AI (see Table 1). The first wave is where the AI works on predefined databases and algorithms, i.e., various databases that are either existing or created humanly or by computers. The further option or course selection is done by the AI by processing of the inputs using the predefined algorithms and comparing them against the databases, and

accordingly generating and selecting options. The first wave AI applications enable reasoning within narrowly defined domains. They have no learning capability and display poor uncertainty handling capability. These systems have been put to successful use in cyber security.[6]

What is becoming mainstream at this stage is the second wave (or the second level) of the AI where the cognitive capability of the computers or their understanding of the external world is utilized for option selection. Machine learning is mostly used for developing the understanding of the external world. The machine learning methods most commonly used are statistical learning and deep learning. In these methods, the AI systems learn to reason by creating statistical data from the inputs they receive from external sources, and by using the limited training data that are fed into these, that is, start "learning" autonomously through training, use, and even user feedback. For example, many commercial applications like Google Maps use external crowdsourcing for correcting and updating information. The use and user feedback enable the AI to refine itself over time.

There are other methods too, such as reinforcement learning. Learning may be "supervised" by humans, where the human assists the machine or "unsupervised" where the AI computer learns to figure out things on its own. For reasoning, the AI tries to group the data using various mathematical techniques built on its neural networks to derive meaningful information like facial recognition, natural language processing, etc. Neural networks are circuits modelled on the human brain and nervous system. Consumer behaviour prediction, and voice and face recognition by the Web apps of Google, Facebook, Baidu, Amazon, etc., are examples of the second wave. Present generation autonomous cars are also part of the second wave of AI.

One limitation of the second wave systems is that an incorrect datafeed over a period of time leads to incorrect learning and training, further resulting in inaccuracies in results. An example is the Microsoft launched software chatbot—"Tay"—designed to learn and respond to tweets. It

---

[6] See "DARPA Perspective on AI", available at https://www.darpa.mil/about-us/darpa-perspective-on-ai, (accessed 16 March 2018).

had to be taken down within 16 hours on account of learning on an incorrect trajectory due to some tweeters teaching offensive and inflammatory tweets to the bot. Overcoming such limitations needs considerable training data input, a tediously huge and impractical effort. Also teaching AI limited things to allow it to learn autonomously from the environmental inputs occasionally may skew the AI and take it into an unrealistic trajectory depending on what kind of inputs are received more frequently. This could make an AI application impractical to function in the real world. The uncertainty negotiation capability of the second wave AI systems is also below the desired mark. This is also reflected in the accuracy levels of cognizance percentages of various AI applications, hardly any of which are above the 70–80 per cent mark at present.

The Third wave of AI, presently under conceptualization, and probably under some experimentation, is AI with contextual adaption. It would have the strengths of both the first wave and second wave systems that would enable it, overtime, to build underlying explanatory models that allow characterization of real world phenomena (much like how humans learn). For example, a cat would be identified as a cat because the computer would identify its certain catlike features as well as its shape, fur, whiskers, claws, ears, etc., and not because of just the overall shape seen in the photograph. This approach would give the AI human like object identification as well as better the power of reasoning, prediction, and intuitive action with better uncertainty handling.[7, 8] Table 1 depicts the characteristics associated with various waves of AI.

Extraordinary Feats

While on one hand the AI employment seems to be getting restrained by issues like uncertainty, on the other hand, AI research having breached the mark of simple problem solving, is now foraying into subjective issues like formulating strategies.

---

7 Ibid.

8 Jane Edwards, "Steven Walker: DARPA Invests in 'Second Wave' AI, Sets Sights on Space Programs", 5 March 2018, available at http://www.executivegov.com/2018/03/steven-walker-darpa-invests-in-second-wave-ai-sets-sights-on-space-programs/, (accessed 06 April 2018).

Table 1: Three Waves of AI

	FIRST WAVE	SECOND WAVE	THIRD WAVE
CHARACT-ERISTICS	• Comparing inputs with predefined algorithms based on rules and databases and generating options accordingly • Reasoning within narrowly defined domains • Poor uncertainty handling and poor performance in uncertain situations	• Uses cognitive capability of the computers or their understanding of the external world • Machine learning methods like cognitive learning and deep learning. • Learns using training data, statistical data creation and user feedback • Neural networks built on human brain model for learning • Uses mathematical techniques to group various data for reasoning, facial recognition • Limited identification and reasoning • Uncertainty handling below desired mark	• Principle of Contextual Adaptation • Systems themselves building underlying explanatory models for reasoning • Most humanlike reasoning power likely • Improved uncertainty handling likely • Limited identification and reasoning • Uncertainty handling below desired mark
APPLI-CATIONS	Cyber security, Chess-Player, Windows Operating System	Facial Recognition, Translation, Natural Language processing, Autonomous cars, gaming computers	Development stage

Source: Author.

The March 2016 victory of the AI computer Google DeepMind using the AlphaGo program in the board game "Go", over the world champion Lee SeDol, which most AI experts believed could not be done for another 15-20 years, really upset the predictions made. The AI made a move so surprising that SeDol had to leave the room for 15 minutes to recover his composure saying, "It's not a human move. I've never seen a human play this move. So beautiful!"[9]

AlphaGo had utilized the deep learning techniques (reinforcement learning), using neural networks by watching thousands of earlier played games to train. In January 2017, an improved AlphaGo version was revealed as the online player "Master" which achieved 60 straight wins in online fast time-control games against top international Go players. In October 2017, Google came out with AlphaGo Zero which was not taught like previous versions but learnt to play the games like Go, Shogi and Chess on its own, playing against itself. It subsequently went on to defeat another advanced AI chess player Stockfish 100-0.[10] The narrow AI is considered to have exceeded the human brain capacity with huge margins in specific fields.

The years 2016 and 2017 brought out many radical AI breakthroughs in the civilian and commercial world, from AI bots evolving their own language to communicate, to AI communication system inventing its own encryption scheme;[11] from robots conducting job interviews,[12] to predicting behaviour of certain people. AI feats are making new headlines almost every day in the media

---

[9] Andrew Ilachinski, "AI, Robots, and Swarms Issues, Questions, and Recommended Studies", *CNA*, Executive Summary, p. v, https://www.cna.org/CNA_files/PDF/DRM-2017-U-014796-Final.pdf, (accessed 13 March 2018).

[10] AlphaGo, "The Story So Far", *Deep Mind*, available at https://deepmind.com/research/alphago/, (accessed 19 March 2018).

[11] Andrew Griffin, "Facebook's AI Robots Shut Down After They Start Talking to Each Other In Their Own Language", *The Independent*, 31 July 2017, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html (accessed 20 March 2018).

[12] "This Russian robot may hire you for your next job", *The Times of India*, 1 April 2018, available at https://timesofindia.indiatimes.com/home/science/this-russian-robot-may-hire-you-for-your-next-job/articleshow/63563841.cms (accessed 3 April 2018).

Table 2: Recent noteworthy applications of AI

FIELD	APPLICATIONS
Transportation	Self-driven vehicles (autonomous trucks, cars, passengers vehicles), metro rail operation, traffic signal operation, route planning and navigation, automatic traffic monitoring and channelizing, fuel efficiency
Health	Managing medical records and other data, analysing tests, X-rays, CT scans, data entry, cancer detection, treatment design and precision medicine, medical consultation based on personal medical history and common medical knowledge, robot assisted surgery, drug discovery, hospital management
Industry	Robotic manufacturing; manufacturing processes control; maintenance activity and shop floor operations optimization; computer modelling and design testing; asset management; supply chain management; inventory management
Education	Adaptation of contents to students' needs, smart content AI tutors, generating teaching models, modelling demonstration
Business	Customer behaviour prediction, demand prediction, virtual assistants to guide customer, secure operations and banking transactions, supply chain optimization, human resource management
Personal Management	Personal schedule tracking requirement prediction, household chores, requirement prediction, power optimization and management, entertainment and media generation according to personal preferences, appointment scheduling

Source: Author.

Table 2 lists some examples of successful applications of AI in the recent times in the civilian sphere.

It would be pertinent here to keep in mind that these breakthroughs do not mean that the technology has been perfected; rather, they indicate that successful forays have been made. As covered earlier, most of these still

need considerable work to be perfected to bring them out as usable applications. They are still experiencing problems mentioned earlier in the text. There are social, ethical and legal aspects also which need to be addressed for each and every AI software application, both in methods and performance, for it to be put to public access and use. These are, however, good to be glanced at, to get a glimpse of what the years ahead have in store. In fact, a search over the internet reveals that the AI is beginning to pervade into every field of human existence. AI is invariably powering all the search engines, spam filters, etc. Virtual personal assistants (like Apple's Siri and Microsoft's Cortana) on the webpages, are using natural language processing in providing web based help. These are fast being adopted by industries and institutions. Industrial robots are almost assaulting the manufacturing sector. It also needs to be kept in mind that though all the remarkable breakthroughs are taking place in the non-military sector, invariably all these have a military offshoot also.

Future Growth and Manifestations

A decade is probably the time period for major impingement in general. Quantum computing, nano-technology and AI are seen to be the symbiotic and synergistic technologies for remodelling mankind's future. A mature "Internet of Things" connect in the near future would integrate AI with formerly inert objects—structures, motors, or appliances - probably giving rise to a supportive parallel for humans. Robotics and autonomous systems are forecasted to underpin the smooth functioning of advanced societies. In fact, a Chinese government document explicitly says,

> AI is going to be the controlling mechanism for most of the future devices and gadgets. Artificial intelligence has become a new focus of international competition. Artificial intelligence is a strategic technology that leads the future. The world's major developed countries regard the development of artificial intelligence as a major strategy for enhancing national competitiveness and safeguarding national security, stepping up planning and policies, and strengthening deployment around core technologies, top talents, and standards.[13]

---

[13] "New Generation Artificial Intelligence Development Planning Notice No. 35 [2017]", *State Council of China*, n. 5.

What has once again come to become a future milestone is the Artificial General Intelligence (AGI) or designing of the machines with human like intelligence and common sense. This is how AI was initially conceptualized. In February 2018, Microsoft co-founder Paul Allen announced that he was investing US $125 million into Allen Institute for Artificial Intelligence over the next three years to fund Project Alexandria, for teaching the machines "common sense", He says, this may take years or decades of work but modern technologies make it easier to build this kind of system.[14] Probably no issue, scientific or subjective or nebulous, would remain outside the purview of the AI then. As AI matures, it would contribute to its own evolution and accelerate the pace of evolution further.

An interesting corollary to the AGI development is that the machines would become self-aware. Experts are more or less unanimously of the view that with the current pace of development, this point in time is still distant. Advanced self-aware AGI has human intelligence and could evolve itself into runaway growth and start pursuing its own goals. The point of crossing called "singularity" (currently forecasted only by 2045 or beyond, at least three decades from now) is hypothesized as a watershed event in human history. It has the potential to lead to existential threat to the human race. Stephen Hawking,[15] Elon Musk[16] and many others have warned about this. Though there are many others who hold opposite views, scientists speculate that the point of singularity also forms a sort of event horizon beyond which it is impossible to predict future happenings. Since this line of exploration and discussion would be a digression from the subject for this research, it is only pertinent to mention here that AI, at

---

[14] Cade Metz, "Paul Allen Wants to Teach Machines Common Sense", *The New York Times*, 28 February 2018, available at https://www.nytimes.com/2018/02/28/technology/paul-allen-ai-common-sense.html, (accessed 22 March 2018).

[15] Hannah Osborne, "Stephen Hawking AI Warning: Artificial Intelligence Could Destroy Civilization", *Newsweek*, 7 November 2017, available at http://www.newsweek.com/stephen-hawking-artificial-intelligence-warning-destroy-civilization-703630 (accessed 9 March 2018).

[16] Javier E. David, "Elon Musk issues a stark warning about AI, calls it a bigger threat than North Korea", *CNBC*, available at https://www.cnbc.com/2017/08/11/elon-musk-issues-a-stark-warning-about-a-i-calls-it-a-bigger-threat-than-north-korea.htm, (accessed 9 March 2018).

its core, is fundamentally unpredictable. It brings in unpredictability of various degrees to any activity, depending on how, and to what extent it is infused in the device, the activity and its environment. How AI will evolve in future cannot be forecasted with certainty. Even experts cannot predict with certainty as to how AI will evolve.[17]

Another corollary, which is rather perturbing, is that with the AI software talent that is burgeoning globally, there is also a threatening possibility of "rogue AI" development in future by malevolently inclined individuals. This could become a sinister tool in the hands of nuisance creators and non-state actors like terrorists. In 2017, "Noel Sharkey, emeritus professor of artificial intelligence and robotics at University of Sheffield [told the House of Lords that]… he feared 'very bad copies' of such weapons—without safeguards built-in to prevent indiscriminate killing—would fall into the hands of terrorist groups".[18] Unlike runaway evolution of the AI, this would be of human creation to bring in a new age terrorism, with its vast and varied dimensions- involving drones, warm attacks, targeting of leaders, tweaking and corruption of existing data structures, etc.[19] A small peek into such future use of AI drones, targeting an individual using face recognition, was recently given by CS Consulting in a demonstration, and is available on the YouTube.[20]

Companies often keep their machine learning applications open sourced and available for universal use. These have a potential to be misused by people to design rouge AI. Public policy researchers from the universities of Cambridge, Oxford and Yale, along with privacy and military experts,

---

17 Andrew Ilachinski, "AI, Robots, and Swarms Issues, Questions, and Recommended Studies", n. 9, Executive Summary, Page xvi, The author cites, "…not even AI experts can predict how AI will evolve in even the near term future much less project its possible course over 10 or more years."

18 Brian Wheeler, "Terrorists 'certain' to get killer robots, says defence giant", 30 November 2017, available at http://www.bbc.com/news/uk-politics-42153140, (accessed 23 March 2018).

19 Ibid.

20 C.S. Consulting, "Micro Drones Killer Arms Robots—Autonomous Artificial Intelligence—Warning!!", *YouTube*, available at https://www.youtube.com/watch?v=TlO2gcs1YvM, (accessed 23 March 2018).

presented a 98 page report warning about malicious use of AI.[21] Adversarial AI attacks to disrupt or take the machine learning of the legitimate AI applications on a wrong trajectory and turn them into misleading or cataclysmic applications, are also the rogue AI manifestations that AI scientists envisage as future challenges. These could be carried out in a number of ways, ranging from physical obfuscation to interfering with the learning process through machine learning attacks.[22] Adversarial learning, however, is also a powerful machine learning tool.

AI Powered Warfare

AI is a potent enabler and has endless possibilities in the military sphere. This is particularly so in the areas where the limits of human intelligence and brain capacities are being reached or exceeded, in processing of data or information using cognitive capabilities. For example, it is used in processing extraordinarily large volumes of data, recognizing patterns therein and deriving meaningful information. The importance of the evaluation and prediction capability of the AI is highlighted by the fact that where the human brain can evaluate and predict the trends of a limited database in one or two dimensions only (as in a graph), AI can make sense of things and make predictions beyond the human imagination. It works in thousands of dimensions, working on real-time huge databases, including multi-dimensional data, and even incorporates the effect of external factors.[23]

---

[21] Eric Auchard, "Artificial Intelligence Poses Risks of Misuse by Hackers, Researchers Say", *Reuters*, 21 February 2018, available at https://www.reuters.com/article/us-cyber-tech/artificial-intelligence-poses-risks-of-misuse-by-hackers-researchers-say-idUSKCN1G503V, (accessed 28 March 2018).

[22] Tristan Greene, "IBM's new AI toolbox puts your deep learning network to the test", *The Next Web*, 18 April 2018, available at https://thenextweb.com/artificial-intelligence/2018/04/17/ibm-launches-open-source-adversarial-robustness-toolbox-for-ai-developers/, (accessed 20 April 2018).

[23] Jim Sterne, "Artificial Intelligence for Marketing: Practical Applications", p. 70, available at https://books.google.co.in/books?id=o_YtDwAAQBAJ&pg=PA78&lpg=PA78&dq=Artificial+intelligence+thousand+dimensional+data&source=bl&ots=g70r6yqbhv&sig=NgpF20b4ZMuzlZm6G75RoHwElGo&hl=en&sa=X&ved=0ahUKEwiDuOqMu47aAhUJOY8KHQX8BgQQ6AEIeTAI#v=onepage&q=Artificial%20intelligence%20thousand%20dimensional%20data&f=false, (accessed 28 March 2018).

The fields in the military sphere which would require such processing in future are intelligence, information and data analysis and distribution, realistic war gaming, prediction, training simulations, communications, logistics, movements, etc. An AI-based logistics system called DART was first tried in 1991 during the Gulf War-1, which DARPA claims had more than paid back their investment.[24]

AI would be particularly valuable in achieving the seamless integration of various sensors and platforms to build clear scenarios for various levels of war control. It would be of assistance right from building grand pictures for the highest levels of controls to exclusively fine-tuned situation presentation for field commanders; from analyzing the situation and generating courses of action and other options, to exercising effective command and control. It would assist in decision making by creating reliability indices for various AI generated courses of action, and could also predict future events for various courses to certain degrees. It could use prediction and pattern recognition to fill in the gaps resulting from fog of war. As covered earlier, AI refining itself over time with usage and feedback would make it more and more trustworthy. At places, a degree of autonomy to the AI in war or battle control, that is, AI taking the decisions, would also find a place in the scheme of things. A major advantage of such AI enabled environment would be shortening of the decision making cycle by reducing the time taken for the activities. Such AI software are likely to be custom made and likely to be in use with the advanced militaries already. However, the use would mostly be classified. One such AI-based system is Roke Manor Research's (Roke) "STARTLE" machine situational awareness software, which would make informed decisions as well as aid in decision making.[25] US Third Offset Strategy also banks heavily on the development of AI, and is effectuating an autonomy driven military-technical revolution. A study, carried out by the US Department of Defense (DoD) in collaboration with a big data and

---

[24] De Spiegeleire et.al, "Artificial Intelligence and the Future of Defence", *n.* 1, p. 35.

[25] "STARTLE", *Roke*, available at https://www.roke.co.uk/what-we-do/intelligent-sensors-and-unmanned-systems/startle, (accessed 4 April 2018).

analytics firm, Govini, mentions, "AI has great potential for creating asymmetric advantages in warfare. Its speed and accuracy in reacting, adapting and predicting scenarios makes it the cornerstone of DoD's Third Offset Strategy."[26]

Force-Multiplier Effect

In-Scenario Building

AI would enable seamless integration of combat field elements like soldiers, vehicles, weapon systems, aircraft, ships, submarines, drones, unmanned vehicles and vessels etc., through one single information base system. It would optimize the data being sent to each and every individual entity on the warfront, attuned to his/its role and requirement. Such integration and effort coordination would have an immense force-multiplier effect, which would not only just be a luxury in complex future war arenas, but an inescapable necessity for success of operations. The definitive advantages of the AI technology would bring a cutting edge, and significant dividends to the side espousing it. In fact, a US Army research paper puts it that without AI infusion, a force may find itself outdated, out-gunned, out-ranged, out-of-position and out-balanced against its adversaries.[27] During the Gulf War-1, information flow was humongous. Information overload was often complained about. As a result, information distribution suffered, even though a tactical information distribution system (the Joint Tactical Information Distribution System) was available.

The wars of the future are expected to be even more information and data intensive, and would invariably need AI superimposed systems. Not only would AI bring in the advantages of well-coordinated military action,

---

[26] "Artificial Intelligence, Big Data and Cloud Taxonomy", *Department of Defense and Govini*, p. 13, available at http://www.govini.com/research-item/dod-artificial-intelligence-and-big-data-taxonomy/?post_title=DoD%20ARTIFICIAL%20INTELLIGENCE%2C%20BIG%20DATA%20AND%20CLOUD%20TAXONOMY, (accessed 12 March 2018).

[27] "The Operational Environment and the Changing Character of Future Warfare", 19 July 2017, available at https://community.apan.org/wg/tradoc-g2/mad-scientist/m/visualizing-multi-domain-battle-2030-2050/200203, (accessed 23 March 2018).

resource allocation, movement and administration, it would also enhance flexibility in case of scenario transformation, unforeseen contingencies or resource degradation. This happens when a new front opens up, a new force is brought in, a force movement is held up/slowed down or there is unexpectedly large attrition. With AI playing its role in integration, the challenge probably would be keeping all entities, data and communication connected during war.

Key Enabler for Multi-Domain Environment

Future conflict environments are hardly likely to precipitate in a conventional war, especially between the major powers. What is envisaged is that the warfare shall be more of undeclared, multi-domain, subversive, and terrorist activity riddled hostilities involving hybrid strategies and grey zone situations, where even most of the military action would take place in complex and densely populated environments.[28] Footprints of this are already visible. Use of unconventional methods like targeting people of specific ethnic masses, leaders and vital installations, using unconventional means and weapons like drones, and cyber warfare is predicted to be the stratagem of future warfare. Invariably, most of such hostilities would fall in the domain of the militaries to counter. This expansion of domain of the military forces from expertise in just the conventional war, to fighting a multifaceted hybrid war, is already taking place, as, elements other than regular forces are seen increasingly playing larger roles during conflicts in the current era. The militaries too are already witnessing increasing demands to expand their scope of operations into other domains of hybrid war.[29]

---

[28] Jerome J. Lademan and J. Alexander Thew, "Objective Metropolis: The Future of Dense Urban Operational Environments", *Modern War Institute*, 2 June 2017, available at https://mwi.usma.edu/objective-metropolis-future-dense-urban-operational-environments/,(accessed 25 March 2018).

[29] Mad Scientist Laboratory, "The Multi-Domain "Dragoon" Squad: A Hyper-enabled Combat System", *US Army Training and Doctrine Command*, available at http://madsciblog.tradoc.army.mil/tag/artificial-intelligence/, (accessed 25 March 2018).

AI systems would be the functional enablers for the forces to operate in the future multi-domain hybrid environments. They would do this by dynamically analysing the situation, figuring out the degree of threat by rationally evaluating different elements in different domains, and assisting in taking decisions in the prevailing nebulosity of hybridity. Modern militaries, like the US, have already started taking the first steps towards readying their field forces for the AI shaped conflict environment of the future, which now does not look beyond the horizon. A blog of the US Army Training and Doctrine Command mentions General Mark Milley, Chief of Staff of the Army, ordering creation of an experimental combat unit known as the Multi-Domain Task Force of the US Army in 2016, equipped with futuristic technology weapons and equipment, including robotics, to study its effectiveness and survivability in future battle environments.[30]

Increasing Impregnation

"Narrow AI" (or AI with limited span of monitoring and action) is already permeating almost all the modern combat battlefield elements such as fighter aircraft, UAV, naval battle systems, marine crafts, battle tanks, missile systems, transportation systems, etc. It is being used to some extent for on board system integration, optimization, sensor fusion and even human triggered weapon launch. It is already bringing a degree of autonomy to many of the tasks the man-machine system is required to perform. Militaries are increasingly employing unmanned vehicles in dull, dirty and dangerous missions like surveillance, reconnaissance, border patrolling, vigil keeping and security, ELINT, communication, terrorist targeting, etc., thus avoiding undue exposure and risk to their personnel. AI can be considered to be in the nascent form in these current military platforms and combat systems vis-à-vis its potential. In time, however, as the AI improves, it would vastly improve and add to the combat capability and survivability of the military systems, and would have to be ignored only at one's own peril. Reports of many military combat and non-combat AI systems under testing keep appearing almost on a daily basis.

---

[30] Ibid.

Autonomous Weapons

Besides the war and battle management systems, AI infused autonomous weapon systems would become field level force multipliers in the future wars. AI would have a major role in the functioning of every major offensive or defensive weapon system of the military. In case of the weapon system this would also include either decision making, or aiding decision making for weapon launch. Autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear arms.[31] It is a point of intense debate whether or not the future lethal autonomous weapon systems (LAWS) should have the weapon launch decision making delegated to the AI. Research on unmanned autonomous combat systems, including advanced battlespace robotic systems, is on a fast track, with developed nations investing considerably in this field, either to retain or gain the combat edge over others. This is likely to lead to the robotic systems becoming increasingly common in their militaries, in the not too distant future. Cases in point are the declared US Third Offset Strategy, and China's AI development plan, which clearly bring out their intention to invest and pursue AI development briskly. Their efforts are discussed later in the paper.

As AI has improved over time, autonomous robotic systems are likely to become very potent platforms for a plethora of missions, in offensive and defensive roles, without risking or putting one's own forces in harm's way. The robotic combat vehicles, that is, various unmanned air, surface, underwater or ground vehicles are envisaged to be game changers in this. AI would enable their combat performance to be made as good as any of the manned combat platforms or may be even better, because of the absence of human limitations like fatigue, G-limitations, etc. Presently, the unmanned combat vehicles are effective mostly in uncontested or well dominated battlespaces because of technology and capability limitations. However, in the future, as AI software improves and technologies like

---

[31] Amitai Etzioni and Oren Etzioni, "Pros and Cons of Autonomous Weapon Systems", *Military Review*, May-June 2017, available at http://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/ (accessed 5 April 2018).

stealth and electronic warfare become more common on unmanned platforms, these would find an increasing role in the contested spaces and active warfronts as well. AI software would be able to effectively engage the enemy's forces using weapons. Robotic systems would be able to skilfully use the terrain, manoeuvre, coordinate, team up with humans, or even operate independently on the warfronts. They could be employed more gainfully for high risk roles, right from Anti-Access/Area Denial (A2/AD) to mine counter-measures; from air-space sanitization and electronic warfare, to combat search and rescue operations.

By dovetailing AI robotic systems with other weapon platforms during offensives, teaming up with soldiers, or forming the first wave of attack, the AI systems would scale down the threat to the assaulting forces. These combat systems could also be used to extend the targeting capability of conventional aircrafts or vessels when carried and launched at the fringe of their radii of action, akin to long range missiles, but with much wider roles and capabilities. As covered earlier, autonomous micro drone swarming or attacking the enemy's fielded forces or airfields in hundreds or thousands, is actively being developed as a warfighting concept and is a promising technology. It is expected to be combat worthy within half to one decade.[32]

AI-based systems would also enable the effects-based operations (EBO) by intelligently targeting selected people and installations, and create desired effects minimizing undue destruction. There are umpteen articles and video footages available on the internet, of other robotic combat concepts that are being worked upon, which seem to present very effective and economical alternatives to the modern expensive weapon systems.

Inescapable Necessity

As AI impregnates more and more military systems, through upgrades or new inductions, the achievement of objectives in military campaigns are likely to become impossible without it. Current systems would become

---

[32] Andrew William Sanders, "Drone Swarms", *United States Army Command and General Staff College*, 2017, available at www.dtic.mil/get-tr-doc/pdf?AD=AD1039921 (accessed 11 April 2018).

obsolete as compared to the new ones in ever shortening time frames, if they are not upgradable. As covered earlier, with the current rate of advancements being made, the major impingement of AI on the militaries is likely to start in about a decade's time. Sceptics often negate, or find it difficult to visualize the enormous difference AI would make to combat capability. They propose that the virtues of human ingenuity would be very difficult to surpass, even by pitching AI systems in military action, especially when combating non-state militia who are increasingly choosing to remain obscure amidst the civilian population.

It is true that AI surpassing human ingenuity is very difficult to envision currently. However, as AI evolves—and features such as face and object recognition are perfected, and the costs involved go down as well—it would be feasible to employ such systems ubiquitously against obscure non-state militia, terrorists or guerrillas, even in populated areas. AI could help identify and predict the locations and hideouts of such militia by putting together and evaluating a number of factors and pieces of information like terrain, population composition, earlier sightings and incidents, their communication, intelligence inputs, etc. This would help to determine their surfacing patterns.

Using AI enabled weapon systems such as drones would selectively target the militia without collateral damage, leaving hardly any space for them to operate. What the sceptics do frequently fail to visualize is the rate of evolution of AI technology, which is exponential. Ray Kurzweil, an MIT graduated computer scientist, a visionary and a celebrated author, in his famous "Law of Accelerating Returns" states:

> The rate of progress of an evolutionary process increases exponentially over time. Over time, the "order" of the information embedded in the evolutionary process (i.e., the measure of how well the information fits a purpose, which in evolution is survival) increases. A correlate of the above observation is that the "returns" of an evolutionary process (e.g., the speed, cost-effectiveness, or overall "power" of a process) increase exponentially over time.[33]"

---

[33] Ray Kurzweil, "The Law of Accelerating Returns", *Kurzweil Accelerating Intelligence*, 7 March 2001, available at http://www.kurzweilai.net/the-law-of-accelerating-returns (accessed 2 April 2018).

Kurzweil has also brought out that humans think of evolution and growth of AI and technology linearly, and make predictions accordingly. They find it difficult to visualize the rapid changes that would occur in future due to exponential growth of technology and the AI.[34] Most of the time, this is the problem with the military visionaries, leading to scepticism against the prowess of AI.

AI military systems, both static and dynamic, would reduce the need for maintaining regular forces and enable downsizing of the militaries. Military expenditure has been on an exponential upswing in most nations, with the compelling necessity of modernization. Thus far, only a few systems are fully automated, and most of them invariably require a human operator in the loop, to various extents. Keeping a human in the loop needs additional systems and human sustenance costs. AI unmanned systems, requiring fewer inbuilt systems, would bring much more economy to military operations as compared to manned systems. They would allow sizeable cuts in costs in equipment, its operation and maintenance. Cummings gives the example of comparative hourly operating costs of the F-22 manned fighter aircraft ($68,362) with the Predator Drone ($3,679), which are almost 18 times in case of the F-22 aircraft. Even if a combat drone is jet engine powered, its operating costs are not likely to exceed half that of the manned fighter aircraft for a similar mission. Employment of small narrow AI drone swarms for the same would cost only a fraction of this.[35]

As a result the US drone industry too has grown tenfold from $283 million in 2000 to $2.9 billion in 2016. One of the reasons of PLAs recently announced downsizing from 2.3 million to below 1 million is to invest the savings for PLA's modernization,[36] which indicates the replaceability of

---

[34] Ray Kurzweil, "The Singularity is Near", *YouTube*, available at https://www.youtube.com/watch?v=y5jiGeQBLTk&t=4323s (accessed 1 April 2018).

[35] Davis Hambling, "If Drone Swarms Are the Future, China May Be Winning", *Popular Mechanics*, 23 December 2016, available at http://www.popularmechanics.com/military/research/a24494/chinese-drones-swarms/ (accessed 11 April 2018).

[36] Adam Ni, "Why China Is Trimming Its Army", *The Diplomat*, 15 July 2017, available at https://thediplomat.com/2017/07/why-china-is-trimming-its-army/ (accessed 5 April 2018).

soldiers with machines. Others may be forced to undertake such measures in the near future as more unmanned systems evolve.

Uncertainty Handling and the Future Wars

The issue of "uncertainty negotiation" which keeps the AI still untrustworthy needs a little more elaboration, particularly from the military usage perspective. Real life situations are full of uncertainties. All the situations of the real world cannot be visualized while formulating rules for the AI. Even in the visualized situations, at times there is so much variance, that it will require a different subset of rules and algorithms for the AI to make the right choices from what have been programmed. Also the external data inputted through various sensors is often corrupted. An AI-based application or system is expected to make out human like sense from it, in spite of the data corruption. Take, for example, a slightly corrupted data (for example, by adding noise) in a photograph of a toothbrush—humans would easily perceive it as a toothbrush, but AI could see it as a baseball bat. Such examples are in plenty where one object has been identified as another similar looking object by the computer. The human mind can still perceive the object correctly in spite of input corruption, but for programming the AI, such problems are big challenges. An autonomous AI car driving through uneven fog or rain, and sensing the traffic through stereoscopic cameras (besides laser and radar ranging gadgets) could easily misidentify the shape, size and direction of objects and traffic on a road. In real life situations, such mistakes could be catastrophic and fatal. The accuracy levels of the current AI systems are still low, for them to be granted full autonomy in critical situations like in AI driven cars in heavy traffic (as there is an additional question of accountability in case of an accident), though they are improving quickly.

When considering AI for employment by the military, what needs to be kept in mind is that battlefields are often riddled with such distortions from smoke, dust, etc. There is also a possibility of adversarial attack corrupting the data to deceive the AI (though the possibility is low due to isolation of pure military systems and networks, and classified source code) The above example mentions one form of uncertainty that is arising from corrupted data from visual sensors, which could affect the action selection process of the AI. Uncertainties for AI from the environment could be

many others, for example, sensor or component failures, or adversarial attacks.

The reason for highlighting the aspect of uncertainty here is because a number of papers are being written and experts are expressing the view (even as late as February 2018) that AI architects are still far from perfecting the uncertainty negotiation. This would prevent fully autonomous AI employment in high risk areas such as self-driven cars, battlefield weapons and platforms, etc., for a long time in future.[37]

In spite of the negative claims of the experts, DARPA claims that it is already using the first and second wave AI to create very powerful platforms, which entails them to reshape defence missions. An example is a recently launched US Navy's first and second wave AI-enabled unmanned ship, which can spend months at sea without human assistance, autonomously maintaining sea lanes, negotiating traffic and carrying out tasks.[38] Another case is the US' continuing testing of various autonomous combat drones in battlefield conditions. For example, in October 2016, a drone swarm comprising of 103 Perdix drones was successfully tested for swarming and mission execution. In the swarm, each of the drones was communicating and coordinating with every other drone, displaying collective and cognitive intelligence in executing tasks, leaderless, somewhat akin to a bird swarm.[39] This successful test is likely to be a precursor to the realistic battlefield trials, and is indicative of a positive nod for autonomous AI in the battlefield.

---

[37] M.L. Cummings, "Artificial Intelligence and the Future of Warfare", *Chatham House*, n. 3, p. 12. The author says, "AI is advancing, but given the current struggle to imbue computers with true knowledge and expert-based behaviours, as well as limitations in perception sensors, it will be many years before AI will be able to approximate human intelligence in high-uncertainty settings—as epitomized by the fog of war."

[38] "DARPA Perspective on AI", n. 6.

[39] Press Release, "Department of Defense Announces Successful Micro-Drone Demonstration", *U.S. Department of Defense*, 09 January 2017, available at https://www.defense.gov/News/News-Releases/News-Release-View/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/, (accessed 16 March 2018).

Some of the Chinese AI drones also have been publicized to have obstacle sensing and avoidance capability through vision sensors, which is a function of cognizance and uncertainty handling, where the AI has to recognize the obstacle and decide how to negotiate it. DJI Phantom 4 Pro is one such drone.[40]

These examples show that while in certain fields, uncertainty resolution may be crucial and cannot be risked, in others, the scenario may not be so muddled and perplexing so as to prohibit the use of autonomous AI devices and vehicles. Safety features can always be incorporated even in the AI, and safety margins can always be laid down while designing or programming the AI for the mission. Even in case of AI driven cars, driving through heavy traffic and in rain may not be tried out at this level of development, but level two AI cars, where there is a driver in the seat and monitoring the behaviour of car, have already been cleared for use in some roads of nations like the US and Australia. In case of uncertainty the car asks the human to take over.[41] Uncertainties arising out of other things like component failures may be not very complicated and difficult to negotiate, as these would have standard failure actions to be followed. At the same time, AI software is also fast being perfected to improve the uncertainty negotiation through techniques mentioned earlier, such as contextual adaption.

---

[40] DJI, "Phantom 4 Pro", available at https://www.dji.com/phantom-4-pro, (accessed 19 March 2018). The brochure says, "Flight Autonomy is expanded with an additional set of high-resolution stereo vision sensors placed at the rear in addition to the pair placed at the front as well as infrared sensing systems placed on the left and right sides. This network creates a total of 5-direction of obstacle sensing and 4-direction of obstacle avoidance, protecting the Phantom 4 Pro from more obstacles and giving filmmakers the confidence to capture more complex images."

[41] Jane Cowan, "Driverless cars: Everything you need to know about the transport revolution", *ABC News*, available at http://www.abc.net.au/news/2017-03-11/everything-you-need-to-know-about-driverless-cars/8336322, (accessed 22 March 2018).

In the context of the role of uncertainties in military employment of AI, the military battlefield scenarios are also not likely to be so perplexing so as to make uncertainty negotiation difficult. Even in a battlefield where autonomous AI drones are being used to attack the enemy, a specific area would be designated to the drones, on the enemy's side. The attacks would be confined to this area, where only military personnel, their equipment and structures would be present, and which would be at a safe distance from one's own forces. No civilian would be expected in that area. The AI drones would use the shape recognition, heat signature, radio emissions or behaviour of the target to select the targets for attacks. Even when the battlefield is riddled with smoke, dust, etc., and there is an uncertainty of clear identification of the target by the AI due to sensor data distortion, the uncertainty will not be a real constraining factor for attacks, since all the targets in that area would be the enemy's. Therefore, the drones could be programmed to press on. Some of the modern weapon systems like Brimstone missile system are already following the principle of autonomously searching and attacking targets in predesignated areas for antitank warfare.[42]

In most of the uncertainties arising in the battlefield due to electronic counter measures, communication signal loss, component failure, etc., which would be only a few, AI could be programmed to press on. Only in a few cases like sensor failure, navigational unit failure, etc., some drones may have to abort the attack. Actions for drones could be programmed depending on the battle tempo and criticality of the battlefield conditions for uncertainty negotiation. Similarly, in an enemy airfield or in a naval battle at sea where only military presence is expected, the uncertainties would be limited. So, in the near future, as the AI software improves, uncertainty negotiation would be better and most uncertainties would not be a prohibitive factor for employment of autonomous AI in battlefields. That is probably the reason why DARPA is moving ahead to develop drone swarms like Perdix, and neither Russia nor China are expected to

---

[42] "Brimstone Air-to-Ground Missile", *Air Force Technology*, available at https://www.airforce-technology.com/projects/brimstone-air-ground-missile/, (accessed 04 April 2018).

hold back on this count. In other scenarios like in anti-terror operations in civilian areas, AI drones may have to be programmed to abort if there is a chance of civilian casualties due to uncertainties. However, as AI software is ameliorated in future, these problems are also expected to be overcome. AI weapons could even be teamed up with one's own forces to make a human-robot force. It also needs to be understood that the issue of uncertainty negotiation is different from delegating the decision to kill to the autonomous weapons. This is discussed further ahead.

However, in warfare, the role of AI would not be limited to controlling drones, or unmanned vehicles/vessels. There are vast applications of AI in the military AI in non-lethal applications are already assisting in many functions, such as navigation, intelligence, scenario building and modelling, simulations, and logistics, etc. Uncertainties are not likely to cause cataclysmic dysfunctionality in these cases, since military systems are likely to be isolated from the civilian internet, and have their own encryption and security measures incorporated in the net environment, with probably a different set of encryptions for wartime. Therefore, the possibility of successful adversarial attack is low. The case of uncertainties—though not unfounded and rather critical for AI application in many of the non-military situations—may not be a disabling or prohibitive factor in most of the military situations and applications. As such there is a 'fog of war' during hostilities, and one of the aims of using AI is to enhance military functionality in such conditions. As examined later in the paper, AI can often help make sense of things in obfuscated or confusing situations.

AI software is being perfected rapidly, and AI is already making forays into autonomy of civilian vehicles and military crafts. The assessment that full AI enabled autonomy is decades away, needs a relook. Autonomous AI-enabled cars are, as such, projected to go into production by 2020.[43] DARPA is in fact working on an AI based autonomous offensive system

---

[43] R.S. Panwar, "Artificial Intelligence in Military Operations: Technology, Ethics and the Indian Perspective", 31 January 2018, available at https://idsa.in/idsacomments/artificial-intelligence-in-military-operations-india_rspanwar_310118, (accessed 28 March 2018).

called Collaborative Operations in Denied Environment (CODE), where multiple drones would carry out entire missions on their own, by assessing environments and situations in real time, often engaging targets on their own.[44]

Additional Challenges

Funding and Organizational Issues

Though AI-based military and warfare systems are probably the most awaited in the military and warfare systems, they are facing some challenges other than developmental ones. Besides uncertainty handling, the major challenge is that of funding for R&D vis-a-vis the commercial sector, resulting in slower development of military AI systems than of non-military systems. Military R&D investment does not bring early returns, and as good dividends, as the commercial sector. Funding to the commercial R&D is supported by many sectors including the software sector, industrial sector, services sector, etc., and is substantially higher than that of military R&D.[45] Funding to defence R&D is mostly restricted to governmental funding, often with constraints of political compulsions, tighter scrutiny, restrictions, etc. Another major factor is that the military usage of technology is seen in a negative perspective by many people, so many good brains are averse to such usage, and prefer to stay away. Cumming further says, 'the global defence industry is falling behind its commercial counterparts in terms of technology innovation, with the gap only widening as the best and brightest engineers move to the commercial sphere.'[46]

There are organizational issues also, which often hamper the development of AI and constrain the funding for the defence AI to mature faster.

---

[44] "Collaborative Operations in Denied Environment", *DARPA Website*, available at https://www.darpa.mil/program/collaborative-operations-in-denied-environment, (accessed 28 March 2018).

[45] Cummings, "Artificial Intelligence and the Future of Warfare", *Chatham House*, n. 3, p. 11.

[46] Ibid.

Cummings points out to organizational in-fighting within USAF and prioritization in favour of manned aircraft, which is impeding the R&D for UAV development.[47] He also says, "For many in the military, UAVs are acceptable only in a support role, as they threaten the status quo if allowed to take the most prestigious, 'tip-of-the-spear' jobs."[48] Creweld writes, "A new weapon may not be accepted because it does not look nice or offer proper room for existing military ceremony."[49] However, in due course, it is expected that the R&D in the defence AI industry will gather pace in the near future, as the global contest for military superiority intensifies. Even commercial sector AI development has a military dimension, as the technology would eventually draw the military's attention. Budgetary allocations for defence sector AI R&D are now on an upswing across the world.

Acceptance of Lethal Autonomous Weapons systems (LAWS)

Before delving into the LAWS issue, it is also important to understand the difference between automated and autonomous systems. An automated system is one in which a computer reasons by a clear if–then–else, rule-based structure, meaning that for each input the system output will always be the same. An autonomous system, on the other hand, may not produce the same results every time. Rather it may exhibit a range of behaviours, which may be different from automated systems as well as other similar autonomous systems, depending how it has learned to perceive things over time. It can independently generate and select among alternative courses of action, to accomplish goals based on its knowledge and understanding of the world around it.

LAWS is a major challenge. Although it seems to provide the foremost advantage of AI for the militaries, there is an intense debate on the issue of empowering non-living entities to decide on causing death and

---

47 Ibid., p. 9.

48 Ibid., p. 9.

49 Martin Van Creveld, "The Invention of Invention", *Technology and War*, p. 223, 1991.

destruction. There is a faction of people including experts and scientists who find it a gross violation of human ethics and norms, and are strongly opposed to such an idea. LAWS, unlike automated systems, must be able to respond to situations that are not pre-programmed or anticipated prior to their deployment. This is where things could go wrong. The issue is not only about the wrong decisions the autonomous AI that could lead to avoidable deaths and use disproportionate force in violation of the international laws, but the likely tendency that may build up in humans, giving up decision making to intelligent machines in future, especially in overloaded and multifaceted conflict environments, which is likely to be devoid of human wisdom. This is also seen by many as morphing into an existential threat for mankind at some stage.

Though most of the experts are opposed to the idea of LAWS, practitioners (defence departments and militaries) are generally moving ahead with the development of autonomous AI lethal systems. This decision would eventually be inescapable, owing to the immediate short term advantages they would bring, or because of the losses that the side may have to suffer by not deploying such weapons, and not delegating destruction and lethality decisions to AI. Stephan De Spiegeleire quotes an example of a 2016 simulated air combat exercise where Psibernetix's artificially intelligent fighter pilot ALPHA soundly defeated US Air Force Colonel (Retd) Gene Lee in a series of simulated dogfights. The "fuzzy logic" based system was able to process sensor data and plan combat moves in less than a millisecond (more than 250 times faster than the eye can blink), while using very little computing power.[50] No nation would like to lose multi-million dollar combat platforms by not opting for autonomy in wars. Task accomplishment using fewer humans, and risk aversion would be other significant advantages of LAWS.

Human in the loop, though desirable and recommended, slows down the decision making cycle. This would become a very critical factor in future warfare and, therefore, may not be acceptable to the strategists and system

---

[50] De Spiegeleire et.al., "Artificial Intelligence and the Future of Defence", *The Hague Centre for Strategic Studies*, n. 1, p. 89.

designers. Even in the US, while critics have often warned against the development of autonomous offensive weaponry for fear of losing operational control, Robert Work, the 32nd US Deputy Secretary of Defense, told CNN that the US pursuit of "narrow AI" will always prioritize human control, but allow the machine to "independently compose and select among different courses of action to accomplish assigned goals based on its knowledge and understanding of the world, itself, and the situation."[51] DARPA is also working on "explainable AI" where in the human-machine interactions, the AI would explain the reasons for making a particular choice, which would help build trust on AI's choices.[52] A *New York Times* report in 2016 mentioned US designing robotic fighter jets to fly into combat alongside manned fighters and missiles that could select targets to attack on its own.[53]

The other major powers—namely, Russia and China—are not so open about their LAWS programmes. In 1995, China had called for legally binding protocol on LAWS. It changed its stance in 2016 and called for responsible use of LAWS, in accordance with the UN Charter and laws of armed conflict.[54] The Chinese government talks about ethos surrounding the use of AI in general, but does not mention the degree of autonomy

---

[51] Zachary Cohen, "US risks losing artificial intelligence arms race to China and Russia", *CNN*, 29 November 2017, available at https://edition.cnn.com/2017/11/29/politics/us-military-artificial-intelligence-russia-china/index.html, (accessed 9 March 2018).

[52] David Gunning, "Explainable Artificial Intelligence (XAI)", *DARPA*, available at https://www.darpa.mil/program/explainable-artificial-intelligence, (accessed 15 March 2018).

[53] Matthew Rosenberg and John Markoff, "The Pentagon's Terminator Conundrum: Robots That Could Kill on Their Own", 25 October 2016, available at https://www.nytimes.com/2016/10/26/us/pentagon-artificial-intelligence-terminator.html, (accessed 5 April 2018).

[54] Bedavyasa Mohanty, "Lethal Autonomous Dragon: China's approach to Artificial Intelligence Weapons", Observer Research Foundation, 15 November 2017, available at https://www.orfonline.org/expert-speak/lethal-autonomous-weapons-dragon-china-approach-artificial-intelligence/, (accessed 20 April 2018).

of the LAWS.[55] These nations, in all likelihood, will go ahead and develop fully autonomous weapon systems out of compulsions of retaining military effectiveness. This may compel even the US to pursue development on a similar trajectory, which to an extent it is already doing by developing CODE and other systems.

There are proponents of the LAWS in the scientific world too, most of whose views are steered by the retaining of military advantages. Pragmatism postulates that fully autonomous weapon systems would, sooner rather than later, see the LAWS materializing, though an option of human-in-the-loop, overseeing things and vetoing AI actions, if required, could be superimposed. Vetoing, once an autonomous platform or weapon is launched, would probably involve either recalling the weapon from its forward position or executing self-destruction, if the system cannot be recalled.

The fog of war often causes wrong identifications and wrong decisions leading to massive unintended casualties at times, even when humans are taking decisions. An example of this is the bombing of the Chinese embassy in Belgrade during the Kosovo conflict in 1999. The situation is only likely to improve with LAWS. Roboticist Ronald C. Arkin believes that with improvement in AI, its decision-making is likely to be superior and more "humane" to that of humans during war. Therefore, the strong argument of ethics against LAWS, that is, delegating decision to AI for the kill, may not find favour with the defence strategists.[56] As such, some autonomous weapon systems are already in use by some militaries. The Harpy (anti-radar missile, offensive role), Iron Dome (rocket/missile interceptor missile, defensive role) of Israel, Phalanx close-in-weapon-system (defensive role) and Patriot missile system (defensive role) of US are some examples. These function with "narrow AI" and are extremely limited in scope vis-à-vis what is envisaged in future.

---

[55] New Generation Artificial Intelligence Development Planning Notice No. 35 [2017], State *Council of China*, n. 5.

[56] Amitai Etzioni and Oren Etzioni," Pros and Cons of Autonomous Weapon Systems", n. 31.

Trust Building

Trust building in the AI system would be another challenge, especially during critical and nebulous situations and particularly for launch of weapons. In spite of the fact that one of the very purposes of AI is supposed to be to guide or take decisions in such situations, due to human nature this will remain a predicament till the time the AI has been checked out, performed several times over and algorithms updated from time to time. The trust is likely to build incrementally and gradually. Another challenge would be preventing AI systems from getting biased and going on a wrong trajectory in assessments or decisions. This could occur during wars due to distortions in information and data, either due to lack of sufficient data resulting from fog of war, or due to information sabotage or even adversarial attacks. This would require authenticating even the real time information and data being inputted, and validating the AI's assessments through duplicacy or triplicacy by different modules using different algorithms, as is done in critical military systems like fly-by-wire system. DARPA also emphasizes on having predictability in machine behaviour,[57] which is another brick in building trustworthiness. The US has proclaimed that they are delving in a big way into AI-based Virtual Reality for training and simulation, and Computer Vision for ISR in the military systems.[58] Alongside, the DoD has also invested in big data processing research and "data hygiene", as the AI is as "intelligent" as the data ingested for processing.

Hardware and Design Challenges

In addition to the above, there are a number of hardware challenges which the military AI systems would have to overcome. These additional challenges transpire from the hostile and destructive military action that these systems have to be designed to face. Military systems have to be necessarily designed catering for battlefield ruggedness, high stress, and

---

[57] "Exhibit R-2: Budget Activity", *Defense Advanced Research Projects Agency*, p. 6, available at http://www.dtic.mil/descriptivesum/Y2017/DARPA/stamped/U_0602303E_2_PB_2017.pdf, (accessed 7 April 2018).

[58] Ibid., p. 13.

rough usage, and they have to have robust fail safe mechanisms. These follow the military standards generally referred to as "Mil Standard" which indicates a tougher build. This kind of designing involves more rigorous testing and much stricter performance guarantees than in the civilian world, which usually takes more time to ensure that the product comes out.

Electronic circuitry and electro-magnetic spectrum dependency of these systems will bring their own set of challenges in trustworthiness, especially for the robotic systems, which would be operating independently and often unconnected. This would involve designing sufficiently durable and reliable power sources, maintaining connectivity, stealth features, resilience against electronic counter measures, virus attacks and electro-magnetic pulse weapons, robustness against hostile action and accidents, etc. The challenges for the AI would be hardening of the systems against EMP and EW attacks, the technology for which would also advance in parallel to the AI and would have the potential to nullify the advantages of the AI systems. A recent example was Iran's bringing down of the US RQ-170 Sentinel drone on 4 December 2011 using EW.[59] Another challenge would be securely retaining connectivity and transferring the information and data to and fro from the battlespace systems, which itself will be subject to many factors like terrain and topography, weather, A2/AD limitations, etc.

Currently, most of the narrow AI applications run on commercially available processors (chips). However, as the AI capability increases in future, it may require much higher processing power using specialized chips. As such, in the commercial sector companies are coming out with Application Specialised Integrated Circuits (ASIC). For example, Google has come out with Tensor Processing Unit (TPU) for its TensorFlow AI framework application.[60] Military technology being restricted, access to such specialized hardware and software could always be denied selectively

---

[59] Nancy Owano, "RQ-170 drone's ambush facts spilled by Iranian engineer", *PHYS.ORG*, 17 December 2011, available at https://phys.org/news/2011-12-rq-drone-ambush-facts-iranian.html, (accessed 8 April 2018).

[60] Massimiliano Versace, "Does Artificial Intelligence Require Specialized Processors?", *The Newstack*, 20 October 2017, available at https://thenewstack.io/ai-hardware-software-dilemma/ (accessed 10 April 2018).

to the nations. One such example is probably IBM's SyNAPSE chip, which was an advanced chip designed in 2014 for DARPA for AI. It was proclaimed loudly then, but is not available anywhere for others to procure.[61] Physical chip designing limitations, that is, the number of transistors that can be placed on a chip, which has already reached a level of nanoscale (e.g., SyNAPSE chip-28 nanometre[62]), may be another limiting factor for future development of AI, until quantum computing can be practically utilized. The powerful processors of AI also would require developing of equally speedy datafeeder and distributor systems (like databuses) and peripherals for AI to function to its capacity.[63]

The Global Leadership Race

The trajectory of the global AI industry is turning parabolically upwards by the day. Global AI research funding in the commercial sector is running into billions of dollars. The global artificial intelligence market size was valued at USD 641.9 million in 2016,[64] which is forecasted to rise to more than $50 billion by 2020,[65] and exceed $15 trillion by 2030.[66] As per one estimate the commercial R&D market is estimated to reach $5 billion by 2020.[67]

---

61 Ibid.

62 Ibid.

63 Ibid.

64 Market Research Report, "Artificial Intelligence Market Analysis By Solution (Hardware, Software, Services), By Technology (Deep Learning, Machine Learning, Natural Language Processing, Machine Vision), By End-use, By Region, and Segment Forecasts, 2018 – 2025", Grand View Research, published in July 2017, available at https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market,(accessed 11 April 2018).

65 News Letter, "Hotify AI to target $5 billion global applied AI R&D market", *ETCIO (initiative of Economic Times*), 24 January 2018, available at https://cio.economictimes.indiatimes.com/news/corporate-news/hotify-ai-to-target-5-billion-global-applied-ai-rd-market/62634429, (accessed 12 April 2018).

66 Sriram Sharma, "Here's why India is likely to lose the AI race", *Factor Daily*, 18 August 2017, available at https://factordaily.com/artificial-intelligence-india/, (accessed 12 April 2018).

67 "Hotify AI to target $5 billion global applied AI R&D market", n. 65.

However, Govini's report quoted US DoD alone spending $7.4 billion in the US fiscal year 2017, on research on cloud computing, big data and artificial intelligence technologies.[68] Joseph DeTrani mentions China committing well-over one hundred billion dollars to AI in its recent five year development plan.[69]

It is amply clear that the current lead nations in the AI research are the US, China and Russia; though EU nations, South Korea and Israel are not very far behind in AI R&D. Distinct governmental initiatives and impetus is now visible in most of the nations. Many piecemeal announcements on AI R&D funding have been proclaimed in the last few years from various quarters of the world. Though investment in defence related AI R&D is classified, with most of the nations, and figures are not available in open source, a substantial investment can easily be adjudged, based on the increasing information about the newer AI projects appearing on the net. The number of research papers on AI has already run into tens of thousands globally.

United States

A multiagency task force created a Networking and Information Technology Research and Development Program, focussing on strategic priorities for information technology (including AI), with particular attention to accelerating the R&D to maintain world leadership, and enhance national defence and security.[70] The US' DoD is currently in the forefront of defence

---

[68] Derek B Johnson, "Pentagon Spending More on Emerging Tech", *Defence Systems*, 5 December 2017, available at https://defensesystems.com/articles/2017/12/06/pentagon-emerging-tech-spend.aspx (accessed 10 April 2018). Ambassador Joseph DeTrani was the President of the Daniel Morgan Graduate School of National Security and prior to that was the President of the Intelligence and National Security Alliance, a professional Think Tank.

[69] Levi Maxey," China's Fourth Industrial Revolution: Artificial Intelligence", *The Cipher Brief*, published on 7 February 2018, available at https://www.thecipherbrief.com/chinas-fourth-industrial-revolution-artificial-intelligence, (accessed 11 April 2018).

[70] Networking and Information Technology Research and Development Program, available at https://www.nitrd.gov/, (accessed 19 April 2018).

AI R&D as a part of its Third Offset Strategy, mainly through DARPA. It has also engaged private corporations like Google, and government contractors like Lockheed Martin, Boeing, etc. To promote novel ideas, and harness the talent of the private sector in AI, DARPA has been conducting a Cyber Grand Challenge for the last one decade, a competition with prize money, which has also been a source of private funding into the AI sector. The US BRAIN initiative is another multi-billion dollar project for AI research over the next decade.[71]

The DoD has instituted numerous studies on AI in the last few years, many of which are available as unclassified documents on the US Defense Technical Information Center (DTIC®) website.[72] The US Army Training and Doctrine Command created a study called "Mad Scientist Laboratory… Forecasting the Future of Warfare", and has been organising brainstorming sessions with scientists and experts titled the "Mad Scientist Conference" to forecast the shape warfare will take in future.[73]

The US has acknowledged, at various instances, the ongoing integration of AI into their various defence systems and confirmed the same. Govini's report says, "the DoD has already begun to integrate AI with mission systems and operating concepts. While the applications are narrowly defined, several years of spending increases provide an indication that AI has gained traction moving beyond test and development phase."[74] In November 2017, the US Deputy Secretary of Defence, Jack Shahanan

---

[71] Shashi Shekhar Vempati, "India and the Artificial Intelligence Revolution", *Carnegie India,* 26 August 2017, available at https://carnegieindia.org/2016/08/11/india-and-artificial-intelligence-revolution-pub-64299 accessed on 12 April 2018.

[72] Defence Technical Information Center, available at http://www.dtic.mil/dtic/search/tr/journal.html, (accessed 10 April 2018).

[73] "Mad Scientist Laboratory", *US Army Training and Doctrine Command*, available at http://madsciblog.tradoc.army.mil/ (accessed 10 April 2018).

[74] "Artificial Intelligence, Big Data and Cloud Taxonomy", *Department of Defense and Govini*, n. 26, p. 12.

indicated the likely availability of the AI technology in the battlefield in 24-36 months.[75]

A cursory look at the various websites related to US DoD, DARPA, etc., and their contracting corporations, namely, Lockheed Martin, Boeing, etc., is a good indicator of the magnitude of US investments in military AI. This spans from information gathering and analysis, to battlefield environment systems, from battlespace weapon technology to military robotics. However, the US is also said to be facing a "Sputnik moment" in AI development with Russia and China according to Robert O. Work himself.[76]

Russia

Both China and Russia have highlighted their intention to pursue AI development vigorously to retain the global balance of economic and military power. However, various Russian statements made acknowledge that their current level robotic technology is lagging vis-à-vis the NATO.[77] While addressing a students' gathering in September, Russian President Vladimir Putin said, "The country that takes the lead in the sphere of computer-based artificial intelligence will rule."[78] He also highlighted that AI will bring threats that are difficult to predict. In January 2017, Putin called for creation of autonomic robotic complexes for the military, with a new National Center for the Development of Robotic Technologies to be established at the Advanced Research Foundation (ARF), the Russian equivalent of DARPA. According to the state media, the Russian military

---

[75] Derek B. Johnson, "Pentagon Spending More on Emerging Tech", 5 December 2017, available at https://defensesystems.com/articles/2017/12/06/pentagon-emerging-tech-spend.aspx, (accessed 6 April 2018).

[76] Zachary Cohen, "US risks losing artificial intelligence arms race to China and Russia", n. 51.

[77] "Back to the future: Putin announced the era of combat robots", *Rambler (Russian)*, 26 January 2017, available athttps://news.rambler.ru/politics/35932393-nazad-v-buduschee-putin-obyavil-eru-boevyh-robotov/, (accessed 12 April 2018).

[78] Zachary Cohen, "US risks losing artificial intelligence arms race to China and Russia", *CNN*, 29 November 2017, n. 51.

is developing AI-based robots, anti-drone systems, border protection systems, and cruise missiles that would be able to analyse radars and make decisions on the altitude, speed and direction of their flight.[79] De Spiegeleire et. al., also quoted from an interview of the General Director of ARF, Andrey Grigoryev, where he corroborated the development of Russian autonomous robotic weapon vehicles.[80] The work further mentioned that while all the current Russian robotic systems had human control, in future Russia may also move onto autonomous systems to match western technology.[81] Russian drone swarming, which needs an AI element, has been reported in various papers.[82]

China

China has a vision to lead the world in AI technologies by 2030, by directly linking defence and commercial development. It also aims to create a share of $150 billion in the commercial market for AI by 2030.[83] In 2017, almost half the global investment into AI start-ups went to China,[84] even though McKinsey analysed in its discussion paper that China does not yet have the same kind of vibrant AI ecosystem as the United States, which has produced substantially more AI start-up companies than China.[85] Most of the experts are coming out with statements forecasting an intense race

---

79 Ibid.

80 De Spiegeleire et.al, "Artificial Intelligence and the Future of Defence", *The Hague Centre for Strategic Studies*, n. 1, p. 82.

81 Ibid., p. 76.

82 United States Army Command, "Drone Swarms", *Kindle Edition,* Chapter 2 [Location 229].

83 "China seeks dominance of global AI industry", *Financial Times*, 16 October 2017, available at https://www.ft.com/content/856753d6-8d31-11e7-a352-e46f43c5825d, (accessed 9 April 2018).

84 Ibid.

85 Discussion Paper, "Artificial Intelligence: Implications For China", McKinsey Global Institute, published in April 2017, available at https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx, (accessed on 13 April 2018).

between China and the US to achieve the lead in AI development over the next decade.[86]

In July 2017, the Chinese government published an unclassified, detailed roadmap outlining a national plan to prioritize the development and application of AI, at the same time accepting that there is still a gap between them and other developed countries in many aspects of AI.[87] The road map elaborately lays down and clearly explains the three steps and six tasks China visualises for AI development. In the first step of the three-step plan, the overall technology and applications of artificial intelligence will be synchronized with the world's advanced level by 2020. The second step is to achieve a major breakthrough in the basic theory of artificial intelligence by 2025, wherein they envisage some of their technologies having reached parity with the world's most advanced. In the third step, by 2030, they envisage the technology and applications to have reached the world's leading level, and China becoming the world's leading artificial intelligence innovation centre, smart economy and smart society. The roadmap highlights the Chinese intention to hawkishly delve into all the facets of AI development, for example, big data intelligence, cross-media awareness computing, human-computer hybrid intelligence (human in the loop), unsupervised learning and comprehensive in-depth reasoning, swarm and group intelligence, and autonomous collaboration and decision-making, etc.

There is a mention of policy tax benefits and incentives for the AI industry, and of encouragement to foreign firms to base their AI development facilities in China. There is no mention of a classified part of the roadmap, as has been proclaimed in the case of the US. However, the document mentions the integration of civilian and military AI programmes, and sharing of civilian and military AI resources, an indication that a classified

---

[86] Levi Maxey, "China's Fourth Industrial Revolution: Artificial Intelligence", *The Cipher Brief*, 7 February 2018, available at https://www.thecipherbrief.com/chinas-fourth-industrial-revolution-artificial-intelligence, (accessed 11 April 2018).

[87] New Generation Artificial Intelligence Development Planning Notice No. 35 [2017], *State Council of China*, n. 5.

section does exist. The tone and tenor of the roadmap could be considered to be aggressive, indicating the high priority the government gives to the technology.[88]

In March 2017, China established its National Engineering Laboratory of Deep Learning Technology under the leadership of Baidu. Many of the Chinese AI-enabled systems are already seeing the light of day. In June 2017, China announced the successful launch of a 119 aerial drone swarm[89] and currently makes a kamikaze drone with explosive warheads.[90] Another milestone which grabbed the media headlines was the commissioning of an AI-based omni surveillance system called Sharp Eyes in March 2018 in 50 cities (which is going to be installed in all of China), having facial recognition and vehicle number plate reading features. This could identify the blacklisted personnel and vehicles in a normal city crowd by instantly comparing them with an existing database, and alert the security personnel. This system not only has facial recognition, but also uses other features such as heat mapping (to identifying crowding), hair styles and clothes for identification.[91] China's AI-based military systems development seems to be much on the same lines as the US.

Others

Not lagging too far behind, Israel, South Korea and the EU have their AI-based border security systems deployed. In 2016, the South Korean government announced plans to invest one trillion won ($840 million) by

---

88 New Generation Artificial Intelligence Development Planning Notice No. 35 [2017], State *Council of China*, Note 5.

89 PTI, "China launches record-breaking drone swarm", *The Economic Times,* 11 June 2017, available at https://economictimes.indiatimes.com/news/international/world-news/china-launches-record-breaking-drone-swarm/articleshow/59095002.cms, (accessed 20 April 2018).

90 Davis Hambling, "If Drone Swarms Are the Future, China May Be Winning," n. 35.

91 Simon Denyer, "China's Watchful Eye", *The Washington Post*, 7 Jan 2018, available at https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/?utm_term=.5617205bfc6e, (accessed 13 March 2018).

2020 to boost its AI industry and major Korean industrial corporations have decided to join the initiative.[92] Their autonomous Samsung Techwin SGR-A1 gun deployed at the North Korean Border, which includes surveillance, tracking, firing, and voice-recognition, often attracts criticism,[93] but nevertheless continues to function.

While Israel has autonomous weapons like Harpy and Iron Dome deployed and a range of UAVs and border patrol vehicles with limited AI faculties operational, it also uses AI-based systems for training. It has plans to have an AI-based decision support system for commanders, and a prediction system to strike time-critical targets.[94]

The EU, through its Seventh Framework Programme, is providing funding for AI defence research[95] and their development programmes are on the same lines as other global leaders.[96] Singapore has committed $150 million for AI research, while the Canadian government is trying to make Canada an AI hub, having more AI talent than the US.[97]

India's Position

India's efforts at AI R&D, particularly defence R&D, are comparatively nascent, and its lag in the field is expressly glaring when viewed with respect

---

92 Lee Chi-Dong, "Gov't to Invest 1 Tln Won in Artificial Intelligence," *Yonhap News Agency*, 17 March 2016, http://english.yonhapnews.co.kr/business/2016/03/17/81/0501000000AEN20160317003751320F.html?bb441f50.

93 "Samsung Techwin SGR-A1 Sentry Guard Robot", *GlobalSecurity.Org*, available at https://www.globalsecurity.org/military/world/rok/sgr-a1.htm, (accessed 11 April 2018).

94 De Spiegeleire et.al, "Artificial Intelligence and the Future of Defence", n. 1, p. 80.

95 Ibid., p. 35.

96 "Launching the European Defence Fund", *European Commission*, 7 June 2017, available at https://eeas.europa.eu/sites/eeas/files/launching_the_european_defence_fund.pdf, (accessed 11 April 2018).

97 Richa Bhatia, "Where does India Stand in the AI race vis-à-vis China, US and rest of the World", *Analytics India*, 18 May 2017, available at https://analyticsindiamag.com/india-stand-ai-race-vis-vis-china-us-rest-world/, (accessed 12 April 2018).

to the size of its economy and defence needs. This is especially so when compared with the state of advancement of its peer powers or even some of the smaller powers. India's current AI industry is estimated to be $180 million annually.[98] According to one study, India had only about 6 per cent of the world's companies and about 29,000 AI professionals in the civilian sector, with just about six-and-a-half years average experience as of 2017.[99] Almost 84 per cent of AI companies in India had less than 50 employees.[100]

In August 2016, Carnegie India published a research paper titled "India and the Artificial Intelligence Revolution"; the paper highlighted the fact that India needs to view AI as a critical element of national security in view of the advancement the world has achieved, and especially in view of neighbour China's rapid progress in the field. The paper also calls India's entry into the domain as "late".[101] The Carnegie paper also reflects that the lag in the AI technology could have serious ramifications, not only in defence, but in all the sectors.[102] It is obvious that a nation will be highly disadvantaged in the near future unless some credible advancements in the crucial sectors of AI and robotics are made.[103] Relying on external technology will not allow India to come close to the lead.

---

98 Digbijay Mishra, "Artificial intelligence task force seeks ₹ 1,200 crore corpus from govt", *The Times of India*, 22 March 2018, available at https://timesofindia.indiatimes.com/trend-tracking/artificial-intelligence-task-force-seeks-1200-crore-corpus-from-govt/articleshow/63409127.cms, (accessed 20 April 2018).

99 Bhasker Gupta, "Study–State of Artificial Intelligence in India 2017", *Analytics India Magazine*, 24 October 2017, available at https://analyticsindiamag.com/study-state-of-artificial-intelligence-in-india-2017/ (accessed 20 April 2018).

100 Ibid.

101 Shashi Shekhar Vempati, "India and the Artificial Intelligence Revolution", *Carnegie India*, n. 71.

102 Ibid.

103 Ibid.

Though Indian private sector companies are harnessed for chip designing, where almost 2,000 chips are being designed every year,[104] chip manufacturing has not picked up in India so far. This is due to the fact that chip manufacturing technology is on the export control list of the US. Some of the advanced chip manufacturing technology has been denied to China too. Though there has been some effort to establish the chip fabrication industry in India which is capital intensive, experts doubt its success due to reasons of overcapacity, profitability and competition.[105] End-toend chip designing and manufacturing, however, are as crucial as in-house AI development from the future cyber security and defence points of view.

There has also been a conspicuous policy support void for the AI sector, though it has now been announced by the Niti Aayog that they would come out with a policy in AI in the near future. This would outline the scope of research and the adoption and commercialization of the technology, to counter China's thrust towards AI. The policy is expected to lay out short, medium and long term goals to be achieved by 2022, 2026 and 2030.[106]

The Government of India also set up a multi-stakeholder task force in February 2018 to formulate a concrete strategy and framework for

---

[104] Anand JI, "Designing Chips For The World", *The Times of India,* 1 October 2017, available at https://timesofindia.indiatimes.com/trend-tracking/designing-chips-for-the-world/articleshow/60894286.cms, (accessed 12 April 2018).

[105] Vinod Dham, "Does India really need a $5bn semiconductor unit?", 21 July 2015, available at https://timesofindia.indiatimes.com/business/india-business/Does-India-really-need-a-5bn-semiconductor-unit/articleshow/48151513.cms?mobile=no#_ga=1.107637570.1745289644.1450296943, (accessed 12 April 2018). In 2016, AMD, world's second largest chip manufacturing giant, has partnered with Hindustan Semiconductor Manufacturing Corporation (HSMC) to help start fabrication in India.

[106] Yogima Seth Sharma, Surabhi Agarwal, "Niti Aayog to come out with national policy on artificial intelligence soon", 21 March 2018, available at https://economictimes.indiatimes.com/news/economy/policy/niti-aayog-to-come-out-with-national-policy-on-artificial-intelligence-soon/articleshow/63387764.cms, (accessed 16 April 2018).

employment of AI in national security and defence needs. The 17-member task force is headed by Tata Sons Chairman, N Chandrasekharan, national cyber security coordinator, Gulshan Rai, academics from the Indian Institutes of Technology (IITs) and the Indian Institute of Science (IISc), representatives from the Indian Space Research Organization (ISRO), the Defence Research and Development Organization (DRDO), the Atomic Energy Commission, and two and three-star military officers. The committee held two meetings on 10 February 2018 and 28 April 2018. A stakeholders' workshop was also held on 21 May 2018. During the workshop, a "Listing of Use Cases" was carried out. The listing is elaborate and includes almost all the areas of AI development or concerns for defence. The list, however, has left out the development of customized hardware (chips) which will be of crucial importance, in future employment of AI.[107]

Though institutions such as the IITs, Birla Institutes of Technology and Science, Delhi University, etc., have been undertaking programmes on AI, there has not been a substantial push in the preceding years, probably due to non-realisation of the potential and the role of AI in future, in all the fields. There have been some small initiatives in developing AI-based applications by the Centre for Advanced Data Computing (CDAC) and the IITs in the civilian sector, but all these efforts can best be termed as entrée level. India's defence AI R&D has primarily been entrusted to Centre for Artificial Intelligence and Robotics (CAIR) under the DRDO. A few small defence and civilian robotic projects are apparently under development, which are listed on their website,[108] but the effort seems insignificant vis-à-vis the scale of development with other players, and future requirements. Wadhwani Institute for Artificial Intelligence, the first AI research institute in India, was inaugurated in Mumbai in February

---

[107] Press Information Bureau, Government of India, Ministry of Defence, 21 May 2018, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=179445, (accessed 22 May 2018).

[108] CAIR, "Products", *Defence Research and Development Organization*, available at https://www.drdo.gov.in/drdo/labs1/CAIR/English/indexnew.jsp?pg=products.jsp, (accessed 12 April 2018).

2018, with a start-up capital of $30 million, though it is dedicated to development of social uses of AI only.[109] In January 2018, an Indo-Japanese collaboration in AI and robotics development in the defence sector was announced.[110] However, any large-scale effort in AI research, and retaining and harnessing the talent in the field is yet to take form.

There has been an awakening to the future manifestations, role and nuances of AI of late, and the Government of India has expressed its intention in various forums, to provide impetus to AI development and take India on the path of global leadership in AI. This also finds a place in the recently unveiled Draft Defence Policy 2018.[111] In the Finance budget for 2018-19, Rs 30730 million ($480 million) have been allocated for the "Digital India" programme.[112] A positive aspect for India is that it has a robust information technology sector, which can become a stepping stone for AI development. However, the effort required would be colossal, as it would also involve creation and retention of talent in India. With the obvious lag that India has had, the Carnegie India paper warns that India may face a near permanent disadvantage in the balance of power against China, with the impetus that China is providing to AI.[113]

---

109 Nilesh Christopher, "India's first AI research institute opened in Mumbai", *The Economic Times*, 20 February 2018, available at https://economictimes.indiatimes.com/tech/ites/indias-first-ai-research-institute-opened-in-mumbai/articleshow/63000704.cms, (accessed 12 April 2018).

110 "India, Japan to introduce AI, robotics in defence sector", *The Times of India*, published on 22 January 2018, available at https://timesofindia.indiatimes.com/india/india-japan-to-introduce-ai-robotics-in-defence-sector/articleshow/62597018.cms, (accessed 12 April 2018).

111 Amit Cowshish, "Promises Galore in the Draft Defence Production Policy 2018", *IDSA,* 2 April 2018, available at https://idsa.in/idsacomments/promises-galore-in-the-draft-defence-production-policy-2018-acowshish-020418, (accessed 12 April 2018).

112 "Budget 2018-2019 Speech of Arun Jaitley, Minister of Finance", Para 109, available at https://www.indiabudget.gov.in/ub2018-19/bs/bs.pdf, (accessed 13 April 2018).

113 Shashi Shekhar Vempati, "India and the Artificial Intelligence Revolution", *Carnegie India,* n. 71.

The Technology Perspective and Capability Roadmap (TPCR) brought out by the Ministry of Defence (MoD) in April 2013, is based on the Long Term Integrated Perspective Plan (LTIPP) of the armed forces, and covers a period of 15 years (the current one is from 2012-2027). It clearly states that the future battlespace will be shaped by technology, and the outcome of future battles will be determined by technology. It emphasizes on self-reliance and ensuring technological developments commensurate with desired military capability.[114] The TPCR only touches very briefly upon application of AI and robotics in the defence sector, such as in image interpretation, maintenance of weapon systems, precision target support, carriage of ammunition and remote fire power. Perspectives have radically altered since 2013, as the immense potential of AI in the defence sector is now being realized, and is being seen as the future game changer in wars. Fresh perspectives have now necessitated a relook at the future technology acquisition and training to make the armed forces future ready, commensurate with all major powers.

Recommendations

Ray Kurzweil has emphasised that if the future impact of AI is to be realized, an exponential growth of technologies and AI will have to be visualized. The landscape is changing quickly and in disruptive ways. As has been discussed earlier in the paper, an increasingly high priority is being given by all the major powers to develop and take the lead in AI based functionality, and the pace of development can only be judged as frantic.

- There is a need to allocate high priority to R&D of AI, AI-based environment and AI-based devices in all the fields including the defence sector, by building a policy support and charting out a roadmap. Not only is there a need to usurp the technology, but there is also a need to periodically review and adjust the policies from time to time, to usher in its benefits to the masses. It also needs to be realised that the periodicity of review would continue to reduce in the future. AI R&D infrastructure creation needs to be given special impetus.

---

[114] "Technology Perspective and Capability Roadmap", *Ministry of Defence*, April 2013 https://mod.gov.in/sites/default/files/TPCR13.pdf, (accessed 14 March 2018).

- There is also a need to provide incentives and stimulus to the chip fabrication and production facilities in the country, and chart out an impetus plan for an accelerated growth of the chip industry, to attain early self-reliance. The current "Make in India" vision and policy already provides a visionary outline for it.

- There is an immediate need to create AI talent by introducing AI in educational institutions, or modifying their educational curriculum to include AI, and at the same time taking policy initiatives, and laying down incentives for retaining the AI talent within the country. Though the finance budget allocates $480 million for Digital India, a substantial allocation needs to be carved out for the AI R&D. As has been seen in the west, the private sector plays a crucial role in AI technology development. Financial incentives in terms of tax benefits and prize money for credible AI applications development needs to be instituted for the AI sector. The partnership of private corporations could be adopted for the defence sector by DRDO, as is being done by other powers. Firstly, it would provide distinct impetus to the R&D; secondly, it would help cover the lag due to late entry; thirdly, it would entice the private sector, which is better at harnessing and retaining the right talent, into AI research; and fourthly, the product is likely to be more competitive.

- There is a need to have periodic technology orientation programmes for the policy makers as well as end users, that is, the defence services, as they often get left behind, due to limited opportunities for exposure, in the day to day running of things. The defence services need to have their own technology monitoring cells, in this age of rapidly changing technology, to assess the effectiveness and impact of newer and upcoming technologies.

- The TPCR lays down the requirement of periodically reviewing the LTIPP due to unpredictability of developments. There have been significant developments in AI and robotics since 2013. The adoption of LAWS, concerns of autonomous weapons systems by the other major powers, is getting addressed gradually and would continue to improve. Experts, policy makers and researchers are coming to the view that LAWS would be inescapable to retain combat edge. It is, thus, the right time to take a relook at these documents.

- There is a need to develop AI-based integrated war management and battle control systems for different levels on priority. These would also include related functions like scenario building, logistics, targeting, intelligence, movements, communications, etc., besides gaming the combat forces. Future warfare would need an integrated approach of the armed forces and non-military elements, to prosecute an AI-enabled environment, and the systems would improve the functionality. Integrated strategies need to be evolved further. AI systems like virtual reality systems, which would cut the costs of peacetime training while making it more realistic and facilitating integration, also need to be given high priority for development.

- AI-based robotics, like unmanned combat platforms and vessels, are likely to accrue distinct advantages for the military in battle action, targeting, collaterals, costs, economy, A2/AD, etc., and needs to be given high priority for development. AI enabled low cost unmanned systems have been viewed as the warfighting tools of the next two to three decades, and their development needs particular impetus. These may radically alter the way battles are fought in the future, particularly in operations like anti-terrorist operations. There is a need to commence work on acquiring and developing LAWS to retain combat edge in the future.

- Development of Non-Nuclear Electromagnetic Pulse (NNEMP) weapons and Electronic Warfare systems and capabilities needs to be given impetus, as the dependency on electronic systems will also see crucial roles of these systems and capabilities.

Conclusion

AI-enabled technology has already started becoming the driver of change for mankind, and its effect is likely to accentuate further in future. This paper concludes with the observation that advances in artificial intelligence have ensured that autonomy has now crossed a "tipping point". There is no alternative to embracing the upcoming technology promptly, and review and adjust the policies to cater for the quick, successive changes that are likely to ensue in future, including in the defence sector.

With the realization of the paramount importance of AI technology, a global contest has already begun, to achieve global leadership in the field.

India's entry into the field of AI development and exploitation has already been delayed, and considering its situation there is a requirement to accord AI development an immediate high priority in order to avoid suffering permanent disadvantage vis-a-vis others, particularly in the defence sector. The way forward for India is a laborious one, as there are multiple challenges right from adopting a forward thinking approach, to drafting policies and roadmap, creating and retaining skill in AI software, creating an industrial base for hardware, and enticing the entrepreneurs to invest into AI software and hardware development. The stirring has already begun but there needs to be a prodigious thrust to catch the required trajectory.

Future war scenarios are likely to be radically different from the past, as there are little chances of a full spectrum war or even a limited war, but the warfare is likely to be hybrid, multi-domain and multi-dimensional, involving very limited military action but more of non-kinetic measures. The nebulous war that is most likely in the future would be highly technology driven. Nonetheless, a nation cannot totally discount the possibility of a major military conflict, and has to keep military preparations at a credible level for it. AI technology will have a central role in war management and controlling the systems whether it is non-kinetic war, hybrid war or a major military conflict. AI technology would have to be fully embraced by all major powers within a decade or two, or at their own peril. India's neighbour, China, boasts of being a leading nation in AI technology and is feverishly working on imbuing AI into all fields including the defence. In such a scenario, autonomous AI military systems and multi-domain capability would be an inescapable necessity for the Indian military. There is still a long way to go in imbuing AI in the defence sector in India. However, it should not be delayed any further lest the disadvantage becomes permanent.

Artificial Intelligence (AI) is emerging as the most disruptive technology of the current era and is advancing exponentially. AI is growing around the concept of machines acquiring human like intelligence for problem solving. Though still in early evolutionary stage, it is already changing the ways the day to day thing are being done. It has already made fair progress and has performed unimaginable feats like natural language processing, facial recognition, multi-dimensional computations and analysis, scientific researches, robotic surgeries, robotic cars, and so many others. No field seems to have been left untouched by this technology. In a decade or so, as the technology evolves further, it is likely to radically transform the ways of the mankind.

AI is also emerging as the base technology for the military systems, where the future intelligent weapons and systems are envisaged to transform the military operations. Intelligent systems are being developed for every possible military field, which include combat, ISR, logistics, transportation, administration, training, etc. Some of these like lethal autonomous weapon systems have raised worries and controversies too. AI, nevertheless, is set to transform and reshape warfare in the near future. This paper analyses the likely reshaping of the future warfare by AI based on current trends of development world over. Looking at the future criticality of technology, the paper also analyses India's position in this whole state of affairs and accordingly makes some recommendations.

Gp Capt Atul Pant is a serving member of the Indian Air Force with 27 years of service and has served in various capacities in the IAF, including instructional tenures and as staff at Air Headquarters. He is currently a research fellow at IDSA.

idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES

Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
E-mail: contactus@idsa.in Website: http://www.idsa.in