An Enduring Dilemma of Artificial Intelligence in the Battlefield

Ravi Srivastava*

Humans have always distinguished themselves from all living beings by virtue of their intelligence. This special distinction has remained undisputed for centuries only to face a major challenge from machines in the form of Artificial Intelligence (AI). This thrilling phenomenon of AI is about the computer algorithms advancing to attain a sizeable quantum of 'inherent knowledge', where they can generate a perspective on issues and produce personalised experiences.[1] In simple words, it is the ability of computer-controlled systems to independently perform tasks, which essentially required human intelligence till now.

AI has now hit the imagination of the current generation. Its arrival on the horizon was anticipated but the technology to sustain it took time to mature. It doesn't have a standalone exclusivity but a complex web of integration with backend systems. AI literally feeds on a dataset, which is not only required to make a referenced decision but also to continuously adjust the outcome as more and more information is made available to the system. So, for an AI-based platform to function user would first need to

* Lt Col Ravi Srivastava, commissioned in the Regiment of Artillery since December 2003, has varied experience of serving in high altitude and field areas, including Rashtriya Rifles, and has held important staff appointments and command tenure in active Counter Insurgency area.

ISSN 0976-1004 (print); 2583-7567 (online)

Journal of Defence Studies, Vol. 18, No. 2, April–June 2024, pp. 149–156

create a massive database to be linked at the backend where the platform would fall back upon encountering a 'query', it will reference from the set of data provided and then come out with an 'average of all' outcomes as its response. Clearly, efficacy of the 'response' would hinge upon the extent and relevance of its connected database.

Walmart was the first commercial venture which attempted to integrate AI in its business payment module in the 1990s. It slowly gained attention and other businesses looked towards adopting AI-based solutions as a cost-cutting tool. It was initially envisaged to replace the massive manpower corporates were sustaining for formulating business analytics, creating future growth modules and handling the company's humongous databases. The AI response was comparatively much faster and more accurate than a human employee if only datasets were to be worked upon. With the launch of Open AI's chatbot Chat GPT[2] in November 2022 and other generative AIs in the competition like BERT and DALL-E, access to this AI tool was easily available to all. It was sudden and before benefits could be realised, the space was quickly filled with deep fakes and plagiarism. It reflected the proverbial tussle between good and evil.

Tech in the Battlefield

As technology advanced, connectivity and integration became the buzzword. Major corporates were rolling out network-supported customer experience. This made anywhere banking, instant payment approvals and live tracking of cargo a possibility. All thanks to the revolution in satellite communication, the advent of the global positioning system and most importantly creation of a networked environment, such as the Internet. These technologies being complimentary to each other took firm roots in late 1900s.[3]

The success soon caught the attention of military strategists; in 1998 Arthur Cebrowski of the US Navy gave a theory of Networked Centric Warfare[4] (NCW). The concept envisaged a Battlefield Command Centre, which will be connected by a stream of networked sensors in all three domains, that is, surface, air and space. These sensors in turn would feed the central database on a real-time basis, the central database using various computing algorithms would quickly be able to sift through voluminous data, which was beyond the realistic capability of human operators. The sifted data would then be filtered based on various pre-defined parameters as the theatre of operation demanded. The filtered data or the 'picture' would be presented to the commanders on the ground to make an informed decision. Since all

this would be automated, the process of data or information evaluation was drastically reduced, shortening the combat decision-making loop.

John Boyd, a USAF pilot and a veteran of the Korean War gave the theory of Observation, Orientation, Decision, and Action (OODA) loop.[5] His argument was, 'it's the speed of the decision making and not the quality of weapons that would affect the outcome in a combat'. The theory was a product of lethal combat results between the F-86 Sabre of the US and the Russian Mig 15 used by the Chinese PLAAF, which was a far superior fighter aircraft during the Korean war. However, the kill results of 3.7 to 1.2 were in favour of F-86. This surprising result was attributed to better cockpit design affording F-86 pilots enhanced view and thus allowing them to make quick decisions during air-to-air duels, as compared to pilots of Mig 15. This theory was a revelation at the time and gained the nod of various military commanders across the world who continuously worked to improve their *kill chain*, *vis-à-vis* their adversary.

The arrival of NCW was another big leap in technology-assisted battlefield management, it was argued that NCW would be a great enabler to commanders on the ground who have information scarcity and combat stress to adequately visualise the true battle picture. It was felt NCW would overcome this challenge with its steady information flow generating quick intelligence assessments for military commanders. The theory was put to test during the Gulf War when for the first time US military was operating in a networked environment.[6] Getting input from multi-layered surveillance sensors and benefitting from analysis of intelligence to speedily react to a developing situation.

Most memories go back to visuals of enemy convoys being picked by satellites, which transmitted live location data to geographically disassociated command centres. The data received in turn was passed onto the nearest fighter aircraft located on a carrier ship which flew in a smart manoeuvre and hit the convoy with GPS-guided bombs achieving pin pointed kill. This was a visual demonstration of the sensor-to-shooter link, shortening the OODA loop and employing the most economical and effective weapons platform enabling battlefield ascendency for frontline commanders.

NCW vs DCW

US 'successful' implementation of an entirely new concept of war fighting in a networked environment was very glitzy and eye-catching. It was also a period of war being broadcast live in our living room. Americans were able to

attain much more as compared to a decade earlier. The percentage of target-observed-target-destroyed and sorties-to-kill-achieved all jumped while relative collateral damage and requirement of troops on the battlefield were reduced considerably. It appeared NCW worked and the US has achieved something its contemporaries had not envisioned till then. This compelled others to come up with similar strategies of their own.

In early 2000, China first gave an insight into how it is planning its military to fight an entirely connected and networked war in the future. Before that, it advocated a doctrine encompassing eight principles, as enumerated in a 1999 book by two PLA officers entitled 'Unrestricted Warfare'.[7] It emphasised strategies a militarily inferior nation can adopt to effectively counter a much superior force. It later came up with the concept of 'Integrated Network Electronic Warfare' (INEW), which envisioned 'Local War Under Informationised Conditions'.[8] China's approach is an integrated response to both Computer Network Attack (CNA) and Electronic Warfare (EW) as an offensive war-fighting tool. Russia followed up soon in 2009, post challenging experience of 2008, in its five-day war with Georgia, Russia announced its 'New Look' strategy.[9] It envisioned '*Setetsentricheskaia Voina*'[10] or a Russian equivalent of NCW. The principle entailed introducing new communication systems boosting existing command and control structures. It integrated the means of reconnaissance, target assignment, and control of troops and weapons, to execute operations in real-time.

However, while the success of the newly formulated NCW was being toasted, US military commanders were also noticing certain disturbing instances brought out at the unit level after action reports, reviews by its DoD and certain post-war analyses by outside agencies. A February 2005 research paper, 'The Challenge And Promise Of Network-Centric Warfare'[11] published by Mr John Luddy on NCW, brought out startling gaps of fratricide instances, missed targets and avoidable collateral damages, which accompanied this new principle. The communication links between sensors, strike platforms and the command centres were not sturdy enough leading to multiple link outages. Limited bandwidth for end-to-end connectivity of so many entities pushed the Pentagon to purchase bandwidth from civilian satellites[12] making them highly vulnerable during military use. The most serious of all challenges noticed in an NCW environment was an 'overload of information with senior commanders, while ground commanders were *still* starved of useful intelligence'. Instances of multiple fratricides due to false IFF shook the operational confidence among forward troops. On 17 February 1991, during the Gulf War, a US Army Air Defence unit fatally

struck a friendly incoming Apache helicopter as it followed on an erroneous radar input.

Such incidents led to enhanced scrutiny of the NCW theory and a better understanding of the pros and cons. By the end of it, NCW gave way to another theory called the DCW or the Decision Centric Warfare.[13] DCW relates to current efforts of creating a Mosaic Warfare harnessing the advantages of superior decision-making speed. It significantly differs from NCW in a way that, for the first time operational planning and executions incorporate AI and autonomous weapons platforms. Also, the US is working towards the development of the Joint All-Domain Command and Control (JADC2), which would use AI for processing data collected by a large number of sensors for supporting ground commanders.[14]

Dark Reality

Howsoever glamorous it may seem, but AI is proving to be a very difficult technology to rely on in combat. Primarily due to its inherent requirement of an almost infinite dataset to emerge as a reasonable responder or act autonomously, especially in complex scenarios as battlegrounds present. AI-enabled platforms would necessarily need a heavy databank for performing the most simple tasks independently such as identification of an enemy aircraft. To understand this complicated scenario, let's look at a future *Autonomous AI Air Defence Weapon Platform*. It would not only require images of all possible aircraft from different perspectives from across the globe to accurately identify but would still be vulnerable to false alarms if combat situations demand dangerous manoeuvres by friendly pilots to deceive the enemy. It may just mark it as a hostile aircraft leading to fratricides.

Another issue that AI-based platforms face is correlation problems. It has been found awkwardly off-mark in identifying practical causes to simple incidents erroneously correlating impractical contexts. An AI system developed for predicting fatalities due to heat waves may reflect an increase in the sale of soft drinks as the likely cause. Now humans know that is totally out of context, but it is very challenging for the machine though. The algorithm would have crunched the datasets as much as it could and 'found' that in summer more and more people getting exposed to extreme climate and suffer heatwave casualty, while summers also increase the soft drink sales. Two remotely correlated but completely out-of-context incidents thus became the important causation for AI. The severity of the problem magnifies multifold as there is no backward means to audit why an AI made a conclusion it did![15]

Correct responses are a logical outcome of correct assessments. For AI systems it is proving incredibly difficult. There have been numerous instances of false positives or false negatives with AI. In simple terms, a false positive is when we are prodded into action where none was warranted and a false negative is when we should have reacted and prodded into inaction. While commercial AI employers can afford to ignore one of the two and focus more on what hurt their capital investment, for military commanders both present fatally dangerous situations.

In a multi-million dollar project undertaken by IBM to revolutionise health care, it developed an AI-supported system Watson for the diagnosis of cancer and suitably recommended the treatment. The idea was to remove the scope of human errors altogether in such a sensitive treatment. Even after IBM's massive investments in R&D and years of trials, the results were uninspiring.[16] The AI-led diagnosis ranged from accurate, and erroneous to outright dangerous the swing of the result was shocking and totally unacceptable. The potent question is, whose error are we prepared to accept: a 'machine error' or a 'human error'? The answer would be of critical interest as the medical treatment is the closest resemblance to combat stress since both are dealing with life-and-death situations. The outcome would likely lead us to answer towards dangers or efficacy of AI on the battlefield.

A New Battlefield

AI nonetheless, is mostly being regarded as an exciting domain in the future of warfare. The vision of an expansive battle zone is minutely covered by four-dimensional deep surveillance, where the networked database is continuously analysing figurative changes fed through all possible sensors. Monitoring enemy losses for working out its logistical endurance, manoeuvres to appreciate forces committed, and intensity of ongoing battle to project additional requirements of reinforcements. Further harnessing and leveraging state-of-the-art autonomous weapons to overcome jamming issues, target high-value enemy assets with almost endless endurance capable deep sea or extremely high-altitude drones. The superbly agile, highly enduring and entirely risk-free machine-controlled autonomous weapons appear to greatly excite military planners today.

However, left to autonomous systems they also offer tremendous risks of miscalculations and disproportionate employment of force. It also appears very scary that AI will make decisions such as pre-emptive strikes to avert major calculative losses, invariably triggering a war by the very action. AI-

supported quick actions for real-time engagements would become the norm, probably even without giving negotiations or diplomacy a chance. Since the chances of error exist, it wouldn't be known if the executed orders are entirely warranted.

Even during the era of NCW, networked war was executed upon dumb adversaries like Iraq or Afghanistan. As the sabotage matrix is equally real, making AI a rather potent liability it would likely restrict its executions to more of a logistical and supportive role rather than full-blown autonomous combat platforms. Modern powers would be wary of executing autonomous machines vs machine combat scenarios that will lead to a non-ending loop with assured mutual destruction. Even some sobering suggestions that AI should only be 'aiding decisions' and not 'taking decisions' will present unexpected decision dilemmas for commanders. Whether or not to rely on AI recommendations on the battlefield, which may be presenting a 'coloured view' or a spoofed result by their sophisticated adversary, a bugged AI is far more dangerous than No AI. The fog of war will be sourced right from command centres by the very machines that were supposedly aiding DCW. The question that will continue to haunt us is—whether it's autonomous AI or human intelligence that should determine the future of war!

Notes

1. 'Get Beyond Basic Personalisation', Artificial Intelligence & Automation Solutions, Genesys, available at https://www.genesys.com/en-sg/capabilities/ai-and-automation?utm_source=bing&utm_campaign=apac_in_dsa_new_searches_002&utm_medium=paidsearch&utm_content=capabilities-call-centre-software&utm_term=en-sg%2Fcapabilities%2Fai-and-automation|b|o|c&mkwid=-dc_pcrid__pkw_en-sg%2Fcapabilities%2Fai-and-automation_pmt_b_slid__pntwk_o&pgrid=1321614624129160&ptaid=dat-2334400624896040:loc-90&msclkid=acddd74c8ac71ad5258eb3b5a56fa97a, accessed on 7 September 2023.
2. 'ChatGPT', Wikipedia, available at https://en.wikipedia.org/wiki/ChatGPT, accessed on 7 September 2023.
3. 'A Brief History of GPS', Aerospace, available at https://aerospace.org/article/brief-history-gps, accessed on 7 September 2023.
4. 'Network-Centric Warfare: Its Origin and Future', USNI, January 1998, available at https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future, accessed on 7 September 2023.
5. 'The OODA Loop and the Half-Beat', *The Strategy Bridge*, 17 March 2020, available at https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat, accessed on 7 September 2023.

6. 'Boosting Network Centric Warfare: View from the Base Level', Bharat Shakti, 5 July 2023, available at https://bharatshakti.in/boosting-network-centric-warfare-view-from-the-base-level/#:~:text=The%201991%20Gulf%20War%20stands,renowned%20for%20their%20combat%20experience, accessed on 7 September 2023.
7. 'Unrestricted Warfare', February 1999, available at https://www.c4i.org/unrestricted.pdf, accessed on 10 September 2023.
8. J. Michael Dahm, 'Electronic Warfare and Signals Intelligence', August 2020, available at https://apps.dtic.mil/sti/trecms/pdf/AD1128255.pdf, accessed on 10 September 2023.
9. 'Russia's "New Look" Military Reforms and Their Impact on Russian Foreign Policy', February 2021, *The International Affairs Review*, available at https://www.iar-gwu.org/blog/2018/02/22/russias-new-look-military-reforms-and-their-impact-on-russian-foreign-policy, accessed on 10 September 2023.
10. 'Tracing Russia's Path to Network-Centric Military Capability',Jamestown, 4 December 2020, available at https://jamestown.org/program/tracing-russias-path-to-network-centric-military-capability/, accessed on 10 September 2023.
11. 'The Challenge and Promise of Network-Centric Warfare', Lexington Institute, February 2005, available at https://www.lexingtoninstitute.org/wp-content/uploads/challenge-promise-network-centric-warfare.pdf, accessed on 10 September 2023.
12. 'Bandwidth Breakthrough', Air and Space Forces, 1 March 2007, available at https://www.airandspaceforces.com/article/0307breakthrough/, accessed on 12 September 2023.
13. 'Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage', Hudson, 3 March 2021, available at https://www.hudson.org/national-security-defense/implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage, accessed on 12 September 2023.
14. 'What Does JADC2 Stand For?', Bae Systems, available at https://www.baesystems.com/en-us/definition/what-does-jadc2-stand-for, accessed on 12 September 2023.
15. 'AI Makes Decisions We Don't Understand. That's a Problem', 19 July 2021, available at https://builtin.com/artificial-intelligence/ai-right-explanation, accessed on 15 September 2023.
16. 'How IBM Watson Overpromised and Underdelivered on AI Health care', Spectrum, 2 April 2019, available at https://spectrum.ieee.org/how-ibm-watson-overpromised-and-underdelivered-on-ai-health-care, accessed on 15 September 2023.