



CENJOWS

CHINA'S ALGORITHMIC
WARFARE:
STRATEGIC IMPLICATIONS OF
AI-DRIVEN MILITARY
OPERATIONS



Wg Cdr Ankit Abbott, is a flying branch officer of IAF. He has commanded a Surface to Air Guided Weapon Squadron.

Introduction

Globally, the buzzwords currently in the technology circle are 'Data', 'Machine Learning', and 'Artificial Intelligence'. The Armed Forces world over are adopting the warfighting tools from different niche technologies. China has also made great strides in this field.¹ The focus is to understand how China leverages AI to augment the capabilities of its armed forces, including but not limited to Intelligence, Surveillance, Reconnaissance (ISR), Autonomous Systems, and Cyber Warfare. Certain essential measures that the Indian Armed Forces must adopt immediately to counter China's advancements are also deliberated upon.

Algorithmic Warfare refers to the use of AI and Machine Learning (ML) algorithms to process vast amounts of data from multiple sources to create a comprehensive picture and, thus, lead to a high level of situational awareness for the military commanders. The algorithms also provide the commanders with automated decisions, thereby, leading to faster response times, optimising the military operations in real-time and precise targeting. All these are shifting the traditional paradigms of warfare to new dimensions.² China has made significant investments in AI-enabled military

technologies, aiming to be the world leader in this crucial domain which could prove critical in changing the outcomes of any future conflict.³

China's Strategic Objectives and Investments in Al-Driven Military Technologies

Chinese government has underscored the importance of AI as the most important pillar on which the modernisation of its armed forces would take place. Chinese government has been providing substantial funding towards research in this field and has issued various policy documents which explicitly bring out its commitment towards the use of AI in military domain. The "New Generation Artificial Intelligence Development Plan," released by the State Council of China in 2017, outlines a comprehensive strategy to make China a global leader in AI by 2030.⁴ This plan highlights the dual-use nature of AI technologies; the use of AI being significantly important in domains of economic development and national security as well.

The erstwhile Strategic Support Force (SSF) - now segregated into Military Aerospace Force (ASF), Cyberspace Force (CSF), Information Support Force (ISF) and Joint Logistics Support Force (JLSF) - of the People's Liberation Army (PLA), which focused on space, cyber and electronic warfare capabilities, had integrated AI into its strategic objectives. The SSF has been instrumental in developing AI applications for military use, ranging from enhancing the ISR capabilities to autonomous weapon systems.⁵ The collaboration between PLA, private industrial sector and academic institutions has further accelerated the pace of development and deployment of AI technologies. Huawei, Baidu and Tencent are few companies who are collocating with leading universities of China and are contributing to advances in AI research in China and its application and employment in military contexts.⁶

China's Technological Advancements in Al-Driven Military Operations

Al-Enabled Intelligence, Surveillance and Reconnaissance (ISR)- The most significant impact of Al-driven technologies has been felt in the field of ISR. Al has enabled data fusion from multiple sources such as satellite imagery, signals intelligence, and human intelligence. This integration of high volume of multifarious data sets is providing a comprehensive and accurate battlefield picture to the commanders on field and at strategic level too. Machine Learning algorithms such as

'Support Vector Machine (SVM)' and 'Neural Networks' are utilised to carry out analysis of ISR data leading to identification of patterns and / or anomalies. For example, 'Convolutional Neural Networks (CNN)' are employed to process and analyse satellite imagery for automated detection and classification of imaged objects with high level of precision.⁸ This capability has proved crucial to process and analyse humongous amount of data collected to monitor movements of the adversary, identification of targets and threat assessment. Additionally, AI driven ISR analytical systems offer real-time analysis which enables military commanders to take faster and better informed decisions. This rapidity of correct decision making, which is aided by real-time analysis of multi-source intelligence, significantly impacts the outcomes of missions. Thus, it can be safely concluded that the use of AI in ISR has enhanced the situational awareness of PLA commanders and provides PLA with a strategic advantage in defensive and offensive operations.⁹

Autonomous Weapon Systems and Drones- The integral components of Algorithmic Warfare are Autonomous Weapon Systems and Drones; an area in which China has made notable progress. These systems leverage capabilities accrued from Al algorithms to perform functions such as navigation, target acquisition and target engagement without human intervention. Autonomous Drones specialise in conduct of Surveillance, Reconnaissance, and Search and Strike missions with high precision.¹⁰ 'Deep Learning' through 'Reinforcement Learning Algorithms' is the key behind the capabilities being exhibited by autonomous drones. These algorithms learn from the environment around them and, thus, the autonomous drones continue to improve their performance over time. The capability of reinforcement learning models can be gauged from the fact the drones equipped with these algorithms can adapt to changing stimuli and optimise their flight paths to avoid detection and maximise mission success. 11 The deployment and employment of autonomous weapon systems raise several strategic and ethical concerns. While the use of these systems greatly enhances the operational capabilities of PLA to rapidly take decisive actions at the strategic and tactical level; however, ethical questions of accountability and the potential for unintended consequences arise from use of Lethal Autonomous Weapon Systems (LAWS). The ethical concerns call for stringent international norms and regulations that must govern the development, deployment and employment of these technologies to ensure their responsible use.¹²

Cyber Warfare Capabilities- Cyber Warfare capabilities of China have seen a quantum jump after imbibing AI. The PLA has been integrating AI in its offensive and defensive cyber operations increasingly. AI-driven cyber tools assist in automating the detection and mitigation of cyber threats, and making cyber defences more robust and responsive to newer threats.¹³ Information Warfare and Psychological Warfare or Cognitive Warfare which are undertaken through means of Cyber Warfare also benefit from integration of AI. The AI algorithms are utilised to analyse social media and other web platforms to identify and counter disinformation campaigns. The AI algorithms are also employed to shape the public perception - own and adversary's - and influence adversarial actions. This capability is particularly relevant in the conduct of hybrid missions where cyber and information operations are combined to achieve strategic objectives.¹⁴

Al-Driven Command and Control (C2) Systems- Al-driven Command and Control Systems (C2) are bringing about a paradigm change in the conduct of military operations by providing Decision Support Systems and enhancing operational efficiency. These systems have the ability to fuse information from multiple sources, analyse them and thereafter present a comprehensive picture of the operational environment, thereby, enhancing the overall situational awareness of the combat commanders. 15 Routine tasks such as data processing and information dissemination have been automated by the Al-enabled C2 systems. This has allowed human operators to focus on strategic decision making. Machine Learning algorithms are predicting potential threats, optimising resource allocation and can even plan military missions. For example, AI can analyse historical data and current intelligence inputs to predict adversary movements and suggest optimal courses of action to combat commanders. 16 The Al-driven C2 systems are also being utilised to facilitate seamless communication and sharing of information amongst different services of the military. These Al driven systems are integrating data from land, air, sea and cyber domains, and creating a unified comprehensive picture of the adversary. This is assisting in high level of situational awareness of the decision makers and is also permitting conduct of coordinated responses to the threats across various domains. 17

Strategic Implications of China's Advancements in Algorithmic Warfare

Shifts in Global Military Balance- The strides made by China in Algorithmic Warfare have shaken the global military balance. The enhanced operational capabilities of PLA due to adoption of Al driven technologies has potentially shifted the power dynamics in key strategic regions - particularly the Asia-Pacific.¹⁸ The substantial advantages gained by PLA in both conventional and asymmetric warfare scenarios - swift decision making, precise targeting and autonomous operations - can be attributed to the abilities accrued from the use of Al systems. The deployment of Al-enabled ISR systems, autonomous weapon platforms and sharpened cyber warfare capabilities can alter the military power calculus of adversaries. These advancements have enabled China to project influence and power beyond its immediate borders; this has been perceived as a challenge to the traditional dominance of the United States of America (USA) and its allies in the region.¹⁹

Risk of Al-Enabled Arms Race- China's brisk pace of development, deployment and employment of Al-driven military technologies has the potential to trigger an Al-enabled arms race among leading world powers. In the great power competition, as nations strive to achieve technological superiority over others, accelerated weaponisation of Al could be resorted to which would lead to increased instability and potential conflicts. Such a competition, to outwit the other technologically, would lead to development of highly advanced autonomous systems which could result in proliferation of lethal autonomous weapons and cyber warfare capabilities.²⁰ An Al arms race could erode the existing international arms control agreements and will present challenges to establishing new international norms on the subject. The lack of transparency and accountability in development and employment further complicates mechanisms to regulate its use - it is easily available to be exploited by both state and non-state actors, and Al clearly has dual-use capabilities. International cooperation through dialogue is essential to develop frameworks for robust governance and prevent misuse and uncontrolled proliferation of Al-enabled weapons.²¹

Implications for Regional Security- Regional security scenarios in the Asia-Pacific and Indian Ocean Region (IOR) would be seriously impacted by China's advancements in algorithmic warfare. The use of AI-enabled military capabilities will alter the strategic behaviour of neighbouring countries and regional actors, influencing

power dynamics and security policies. Utilising the abilities of Al-enhanced ISR systems, autonomous drones, etc. China would be able to monitor, patrol and control the South China Sea, which it claims is vital to it. The Taiwan Strait is another flashpoint where China could significantly alter the security landscape by exercising its advancements in algorithmic warfare. PLA could enhance its preparedness for likely military operations in the Taiwan Straits and develop contingency plans based on the results of simulations of multiple conflict scenarios carried out through high-end Al algorithms.²² The enhancement in PLA's capabilities would challenge the strategic interests of Japan, South Korea and Australia too, amongst other South-East Asian countries. Al-enabled systems provide China with capabilities to swiftly detect and respond to any perceived threat or unauthorised activities by other claimant nations or external powers like the USA.23 The increased capability for precision targeting and real-time battlefield management supported by Al-enabled systems could lower the threshold for military action by China, as the PLA might feel more confident in its abilities to achieve swift and decisive victories with minimal collateral damage. This potential for rapid escalation poses significant risks to regional security and could lead to broader conflicts involving other regional powers and the USA, which has committed to supporting Taiwan's defense.²⁴ It is well understood that China's capability to leverage AI to enhance information warfare and conduct economic coercion and cyber operations, could be utilised towards creating complex challenges for regional security and stability, and the nations in the region must always be on guard against these.²⁵

Security Implications for India- China's giant strides in algorithmic warfare pose significant security concerns for India. India is a key regional actor and its rise in global power index is not going down well with China. The balance of power along the unsettled Indo-China border and in the Indian Ocean, which is already on shaky grounds after the incident at Galwan in year 2020, will transpose as China enhances its capabilities through Al-driven technologies. The superior ISR-enabled situational awareness, decision support through Al-enabled systems and capability to respond swiftly could significantly undermine India's security position. Moreover, use of Al in domain awareness, whether maritime or air, would improve China's ability to conduct Anti-Access Area Denial (A2AD) operations. Further complications in India's defense strategies would arise due to the increased precision and efficiency of Chinese military operations. This necessitates a substantial upgrade in the technological prowess of Indian armed forces. China's progress in cyber warfare, bolstered by Al, presents a

direct threat to India, especially its critical infrastructure including defense communication networks which could be targeted to disrupt military communications, and command and control systems during any conflict. The overall threat faced by India is further exacerbated by China's potential to use AI for asymmetric warfare tactics like cyber espionage and information warfare.²⁶ These could be used to destabilise India's internal security environment through the spread of negative propaganda and disinformation campaigns. These threats make it incumbent for India to invest in robust countermeasures.²⁷

International Responses and Policy Considerations- In response to China's advancements in algorithmic warfare, the international community must enhance its own AI capabilities and develop comprehensive strategies to address associated challenges. This would include investing in research and development on AI, fostering public-private partnerships on the issue and promoting international cooperation on AI governance.²⁸ Since this technology is dual-use and has a vast scope of utility in the civil domain, policy considerations on the subject must focus specifically on international norms and regulations to govern the use of AI in the domain of armed conflict. Transparency, Accountability, and Ethical Considerations must be the pillars on which this framework should be developed. While the international community progresses with its development of AI-enabled systems for use in conflicts, as a response to China's developments, collaborated efforts must be made to prevent an AI Arms Race and ensure its responsible use towards maintaining global security and stability.²⁹

Ethical Considerations and Human Oversight in Algorithmic Warfare

Ethical Dilemmas- Integration of AI into military operations raises certain ethical dilemmas. While AI-driven systems can provide decisions faster than any human being, however, concerns about their accuracy, accountability, and most importantly, the morality of the decision cannot be overlooked. The simplest example to understand these ethical concerns is the delegation of life and death decision to a machine by deployment of a Lethal Autonomous Weapon System (LAWS) in a conflict zone wherein it will enjoy complete autonomy in taking and executing the decision. Oncerns arising about the potential of AI systems to perpetuate biases or making erroneous decisions due to flawed algorithms or insufficient data need to be

deliberated and addressed. Such errors in an AI system deployed in a battle zone could lead to unintended casualties and / or collateral damage. These are some of the most important questions that are raised about the ethical use of AI in combat operations.

The Importance of Human Oversight- Human oversight on Al-driven military operations will remain the paramount safeguard in addressing the ethical challenges brought out above. All may process vast amount of data from varied sources and produce the output after performing complex tasks; it is the human in the loop who must use his / her judgement to make the final decision after careful interpretation of the All generated result. This would ensure that the ethical considerations of employment of Al-driven systems are catered to and that the accountability of decisions is maintained. Human oversight through 'Human-in-the-Loop', keeps the boundaries of use of All in military conflict in control and ensures that indiscriminate use of All, without ethical considerations, does not take place. This includes defining the roles and responsibilities of All systems, laying down clear rules of engagement, and ensuring that human operators retain final control over ethical decisions. Robust oversight mechanisms can help mitigate the risks associated with All and ensure its responsible use in armed conflict. Place in addressing the ethical challenges and produce and

Governance and Regulation- To address the ethical and strategic challenges posed by these technologies, it is essential that suitable governance frameworks and regulations are developed. International community must come together and lay down agreements and norms that provide clear guidelines for the development and deployment of Al-driven systems in armed conflict. International cooperation is crucial to developing these frameworks and ensuring their effective implementation.³³

What Indian Armed Forces Must Do

The increasing integration of AI and advanced technologies into China's military operations poses substantial challenges to the Indian Armed Forces, necessitating adoption of robust countermeasures. Action points listed in subsequent paragraphs outline essential steps that the Indian Armed Forces must take to enhance their technological prowess and strengthen cybersecurity which would ensure strategic parity with China. Through implementation of these measures, India would be able to

counter potential threats, fortify its defensive posture and be able to maintain competitive edge in the era of rapid technological evolution.

Enhance ISR Capabilities- Develop and deploy advanced ISR systems, incorporating AI and Machine Learning, which are able to fuse data inputs from multiple sources of all the services and other national agencies, and produce a unified comprehensive situational awareness picture after analysis of the fused data. The system should possess capabilities of 'Classification' of objects, 'Change Detection', and 'Predictive Analysis' of likely future dispositions of the adversary.

Decision Support Systems- Integrate AI into existing defense platforms and systems to provide decision support to on-scene commanders through front-edge computing. Further, these front-edge systems should be connected to a C2 centre at the rear where AI-driven decision support systems are running to provide decision support to operational and strategic commanders.

Strengthen Cybersecurity Infrastructure- Implement AI-enabled robust cybersecurity measures to protect critical infrastructure, military communication networks, and C2 systems. Defence Cyber Agency must lead the way in this regard.

Focus on Asymmetric Warfare Tactics- Form a nodal agency to develop and employ asymmetric warfare tactics leveraging AI for cyber espionage, information warfare, and psychological warfare to counterbalance China's advances in this domain.

Autonomous Unmanned Combat Aerial Vehicles- A large number of start-ups have forayed into small-scale drones and drone swarms with varying levels of autonomy. The urgent need for a fully autonomous unmanned combat aerial vehicle must be addressed through collaboration between defense PSU, private industry, and academia with IAF in the lead to drive the project. With suitable upgrades and data linking, this would also fill the futuristic requirement of Manned-Unmanned Teaming for the next generation aircraft.

Invest in Al and Cyber Capabilities- Tri-service integrated single nodal agency must be formed to formulate and lay down the trajectory of Al development for Indian Armed

Forces. In collaboration with private industry and academia, this agency must invest in R&D in AI to enhance India's capabilities in algorithmic warfare.

Enhance International Cooperation on Al- Indian Armed Forces, through suitable frameworks, must strengthen strategic partnerships and collaborations with countries at the forefront of Al research, to conduct joint research, training and Al-enabled military exercises.

Conclusion

The integration of AI and advanced algorithms in the conduct of military operations represents a marked shift in modern warfare. AI-driven technologies, while providing considerable strategic advantages, present ethical, legal, and strategic challenges too.

China's capabilities in the domain of algorithmic warfare have reasonably advanced. This has resulted in increased capabilities affecting the global security scenario. This has implications for India as well as those countries having a stake in India Ocean Region and Indo- Pacific.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

¹ "In One Key A.I. Metric, China Pulls Ahead of the U.S.: Talent", The New York Times, accessed May 25, 2024, https://www.nytimes.com/2024/03/22/technology/china-ai-talent.html.

² Allen, Thomas. "Artificial Intelligence and National Security." Harvard Kennedy School Belfer Center for Science and International Affairs, April 2020.

³ Kania, Elsa B. "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power." Center for a New American Security, November 2019.

⁴ State Council of China. "New Generation Artificial Intelligence Development Plan." July 20, 2017.

- ⁵ "The PLA's Strategic Support Force and Al Innovation", Brookings, accessed May 25, 2024, https://www.brookings.edu/articles/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/.
- ⁶ "Deciphering China's AI Dream", Future of Humanity Institute, University of Oxford, accessed May 25, 2024, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.
- ⁷ Kania, Elsa B. "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power." Center for a New American Security, November 2019.
- ⁸ Tanya Jain, Mohd Jawed Khan, Shubham Pandey, Shivam Mishra, Shubham Yadav, "Satellite Image Classification and Analysis using Machine Learning with ISRO LISS IV", International Research Journal of Engineering and Technology (IRJET), Volume: 09 Issue: 05 (May 2022), https://www.irjet.net/archives/V9/i5/IRJET-V9I5402.pdf.
- ⁹ Cheung, T. M. (2011). The Chinese Defense Economy's Long March from Imitation to Innovation. *Journal of Strategic Studies*, *34*(3), 325–354. https://doi.org/10.1080/01402390.2011.574976.
- ¹⁰ "Military Applications of Drones: Surveillance, Reconnaissance, and Beyond", AV8prep, accessed May 25, 2024, https://www.av8prep.com/aviation-library/part-107-drone/military-applications-of-drones-surveillance-reconnaissance-and-beyond.
- ¹¹ Kalidas, Amudhini P., Christy Jackson Joshua, Abdul Quadir Md, Shakila Basheer, Senthilkumar Mohan, and Sapiah Sakri. 2023. "Deep Reinforcement Learning for Vision-Based Navigation of UAVs in Avoiding Stationary and Mobile Obstacles" *Drones* 7, no. 4: 245. https://doi.org/10.3390/drones7040245.
- ¹² Asaro, Peter. "Al Ethics in Predictive Policing: From Models of Threat to an Ethics of Care." IEEE Technology and Society Magazine 38, no. 2 (2019): 40-53.
- ¹³ "Role of Artificial Intelligence (AI) in Cybersecurity", Fortinet, accessed May 25, 2024, https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity.
- ¹⁴ Ilyas, Muhammad. (2023). "The Impact of Artificial Intelligence on hybrid warfare: Case of Russia-Ukraine war", Journal of Liaoning Technical University (Natural Science Edition) 17. 01-22. https://www.researchgate.net/publication/375164694_The_Impact_of_Artificial_Intelligence_on_hybrid_warfare Case of Russia-Ukraine war.
- ¹⁵ Kania, Elsa B. "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power." Center for a New American Security, November 2019.
- ¹⁶ "Data Analytics in the Combatant Command: Improving the Approach to Decision-Making", Strategy Bridge, accessed May 26, 2024, https://thestrategybridge.org/the-bridge/2021/9/6/data-analytics-in-the-combatant-command-improving-the-approach-to-decision-making.
- ¹⁷ "Deciphering China's Al Dream", Future of Humanity Institute, University of Oxford, accessed May 25, 2024, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_Al-Dream.pdf.
- ¹⁸ "China's Military Employment of Artificial Intelligence and Its Security Implications", The International Affairs Review, accessed May 26, 2024, https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap#:~:text=SECURITY%20IMPLICATIONS%20OF%20CHINESE%20MILITARY'S%20EMPLOYMEN T%20OF%20Al&text=For%20a%20region%20that%20is,concerning%20autonomous%20lethal%20wea pon%20systems.
- ¹⁹ Horowitz, Michael C. "The Promise and Peril of Military Applications of Artificial Intelligence." Bulletin of the Atomic Scientists 74, no. 2 (2018): 96-101.
- ²⁰ "The AI arms race has us on the road to Armageddon", VentureBeat, accessed May 26, 2024, https://venturebeat.com/ai/the-ai-arms-race-has-us-on-the-road-to-armageddon/.
- ²¹ Scharre, Paul. Army of None: Autonomous Weapons and the Future of War. W.W. Norton & Company, 2020.
- ²² Davis PK, Bracken P. "Artificial Intelligence for Wargaming and Modeling". The Journal of Defense Modeling and Simulation. 2022;0(0). doi:10.1177/15485129211073126.
- ²³ "China's Military Employment of Artificial Intelligence and Its Security Implications", The International Affairs Review, accessed May 26, 2024, https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap#:~:text=SECURITY%20IMPLICATIONS%20OF%20CHINESE%20MILITARY'S%20EMPLOYMEN T%20OF%20Al&text=For%20a%20region%20that%20is,concerning%20autonomous%20lethal%20wea pon%20systems.

- ²⁴ "Official Says U.S. Committed to Taiwan's Defense ", U.S. Indo-Pacific Command, accessed May 26, 2024, https://www.pacom.mil/Media/News/News-Article-View/Article/3221924/official-says-us-committed-to-taiwans-defense/.
- ²⁵ "Al Frontlines: China's PLA Evolution vs. NATO's Counterplay", Friedrich Naumann Foundation for Freedom, accessed May 26, 2024, https://www.freiheit.org/taiwan/ai-frontlines-chinas-pla-evolution-vs-natos-counterplay.
- ²⁶ Horowitz, Michael C. "The Promise and Peril of Military Applications of Artificial Intelligence." Bulletin of the Atomic Scientists 74, no. 2 (2018): 96-101.
- ²⁷ Kania, Elsa B. "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power." Center for a New American Security, November 2019.
- ²⁸ Allen, Thomas. "Artificial Intelligence and National Security." Harvard Kennedy School Belfer Center for Science and International Affairs, April 2020.
- ²⁹ Asaro, Peter. "Al Ethics in Predictive Policing: From Models of Threat to an Ethics of Care." IEEE Technology and Society Magazine 38, no. 2 (2019): 40-53.
- ³⁰ Asaro, Peter. "Al Ethics in Predictive Policing: From Models of Threat to an Ethics of Care." IEEE Technology and Society Magazine 38, no. 2 (2019): 40-53.
- ³¹ Scharre, Paul. Army of None: Autonomous Weapons and the Future of War. W.W. Norton & Company, 2020.
- ³² Horowitz, Michael C. "The Promise and Peril of Military Applications of Artificial Intelligence." Bulletin of the Atomic Scientists 74, no. 2 (2018): 96-101.
- ³³ Asaro, Peter. "Al Ethics in Predictive Policing: From Models of Threat to an Ethics of Care." IEEE Technology and Society Magazine 38, no. 2 (2019): 40-53.