AI-Driven Command and Control for Rapid Response to Multi-Vector Attack: Enhancing Military Operations

Shipra Gupta

INTRODUCTION: ARTIFICIAL INTELLIGENCE (AI) SUPREMACY IN RESHAPING BATTLEFIELD SCENARIO

With the advent of technology and the present pace of automated integration, the ways and means available with a state to attack another have increased considerably. The battlefield is modernising and fetching additional complications, with adversaries employing a range of tactics and technologies to gain strategic advantage. The need for a rapid response to multi-vector attacks has become a critical component of military planning. Automation of such operations is inevitable to enable quick adaptation to the changing circumstances, and respond to emerging threats for safeguarding national assets.

Squadron Leader **Shipra Gupta** is a serving officer of the Indian Air Force and presently serving at the Air Defence College.

According to the International Joint Conference on Artificial Intelligence (AI) (July 2015):

> AI technology has reached a point where the deployment of [autonomous weapons] is—practically, if not legally—feasible within years, not decades, and the stakes are high: autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear arms.[1]

The evolving technology of automation is reshaping modern warfare, driving a transformation in how militaries organise, train and fight. It is understood worldwide that AI will soon dominate the combat zone and has the power to shape or modify the perception, planning and, thereafter, the execution, of complex operations. In an era where threats span multiple domains—ranging from the physical, electrical, biological, information, cyber and nuclear—success will decidedly rely on the speed and precision of the response. The conventional means of command and control to tackle any threat often scuffle to balance out the pace and density of these evolving challenges.

The AI-driven command and control system will offer pragmatic solutions by integrating multiple facets of decision-making and analytical tools. Such systems would enhance situational awareness, data processing and assessment of multiple scenarios at unprecedented speed. In view of this precept, the article explores the role of AI-driven command and control in enhancing military operations, with a focus on rapid response to multi-vector attacks.

1. A letter signed by Elon Musk, Stephen Hawking, Steve Woznaik and over 1,000 AI researchers, presented at the International Joint Conference on Artificial Intelligence, July 2015.

Non-Conventional Means of Multi-Vector Attacks: Complex Problems Require Modern Solutions

In military parlance, a multi-vector attack refers to a coordinated assault that strikes a target from multiple directions or domains simultaneously. In today's scenario, such assaults may utilise various spectra: land, air, space or marine; or different vectors: cyber, electronic warfare, and kinetic attacks, to overwhelm an adversary's defences and disrupt its command and control structures. These attacks may be simultaneous or the best match to complement the generation of asymmetry at the designated target area. Such attacks aim to be highly penetrative into the defensive layers by creating chaos and confusion, making it difficult for the adversary to respond effectively.

Many scholars claim that multi-vector attacks come with challenges of their own. Spontaneity, lethality and the surprise element further complicate the scenario, leaving little time to decide and react. Moreover, the technological progress has made some traditionally uncontested domains like space more contested; created new, more competitive domains like cyber; and increased the complexity of some environments like information, which, in the meantime, have come to play an even more important role.[2]

Challenges: There are numerous challenges in dealing with multi-vector attacks.

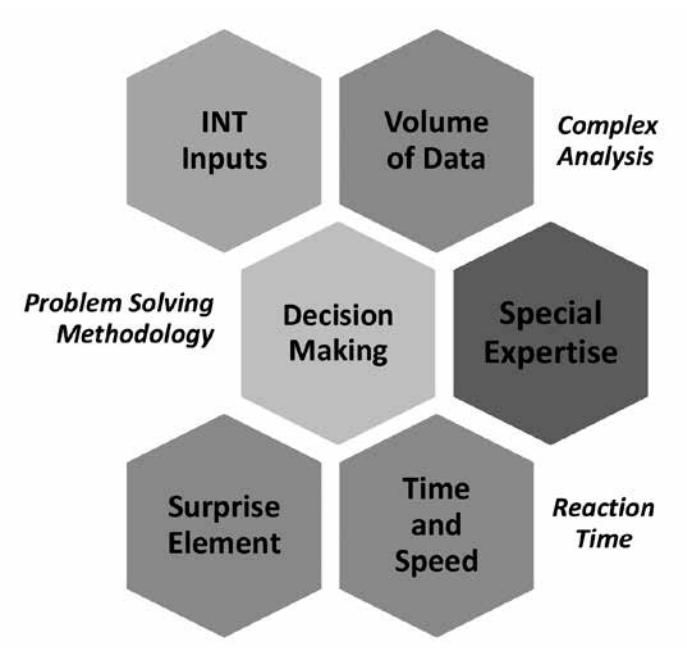
- Firstly, the humungous amount of data pertaining to numerous permutations and combinations generated by these attacks can be overwhelming. It becomes highly demanding to be analysed by the human brain or brainstorming by multiple decision-makers to present favourable results within a few seconds.

2. T.C. Rid and M.Hecker, *War 2.0: Irregular Warfare in the Information Age* (Praeger, 2009); B. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Harvard University Press, 2020); Defence Intelligence Agency, *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion* (Washington, DC: Department of Defence, 2022).

- Secondly, the speed at which these attacks unfold, leaving little time for decision-makers to respond. The aspect of surprise, reaction time of the existing Air Defence (AD) chain, quality of intelligence inputs, and degree of its augmentation in the AD layers further affect this attribute.
- Lastly, the complexity of these attacks can be high, requiring specialised expertise to understand, and respond to, the various vectors involved. Understanding of multi-domain operations requires advanced capabilities in all domains and advanced holistic knowledge of their effects.[3]

Thus, to deal with the challenges, thorough digitisation of the decision and solution process is required.

Fig 1: Challenges of Multi-Vector Attacks



3. Andrea Gilli, "NATO, Multi-Domain Operations and the Future of the Atlantic Alliance", research article, published on January 14, 2025.

Augmenting AI to Combat Multi-Vector Attacks: Prompt and Simplified Outcome

The solution to any problem commences with an analysis of the various situations and matching it to the best result. AI can be used to analyse these scenarios associated with vast amounts of data in real-time, identify patterns and anomalies, and provide decision-makers with critical information to augment their decisions towards success.

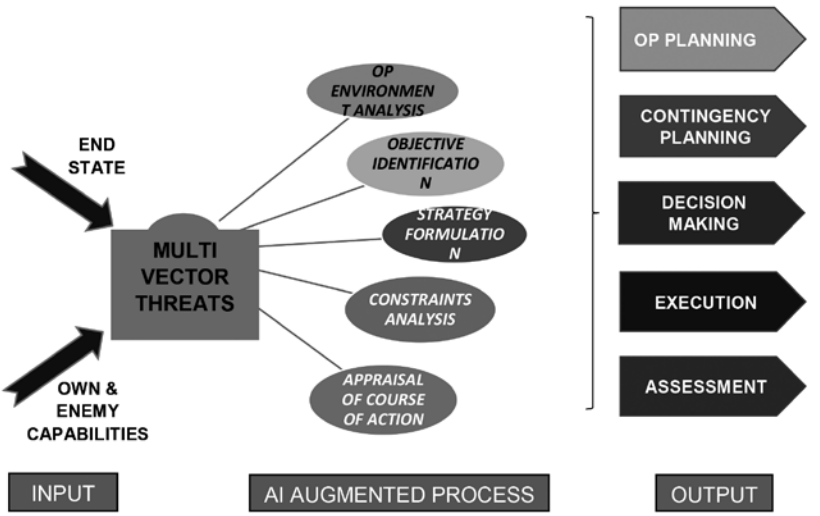
In the context of military organisations AI can play a crucial role in several areas. AI can assist to tackle multi-domain and multi-vector attacks by enabling rapid data integration, cataloguing of information and data analysis, enhancing Situational Awareness (SA) and improving Spare Mental Capacity (SMC).

Addressing a multi-vector threat through AI would require automation of certain planning and decision-making steps. The planning process would involve identification of the military end state, operational environment analysis, evaluation of own and enemy capabilities/intentions, objective identification and effect determination, strategy formulation, identification of the most likely Course of Action (CoA), operational plan preparation and contingency planning.[4] The execution of the most apt tactical action and the assessment of the result, with the associated feedback, would follow afterwards.

AI has the potential to revolutionise Command and Control (C2) in military operations, enabling a rapid response to multi-vector attacks and enhancing the effectiveness of military operations. Let us dwell on the key segments, where AI can be utilised in combating multi-vector threats.

4. Operational Doctrine of the Indian Air Force: IAP 2000-07 Part II (Restricted Document published in 2007).

Fig 2: Use of AI to Address Multi-Vector Attacks



- **Threat Detection and Identification.** AI can recognise the characteristics of various attack vectors with respect to the given target system. The processing would require a data repository of target characteristics—own and adversary capabilities—which can further be refined via Machine Learning (ML) in due course of time. AI can quickly process and analyse large amounts of data from various sources, including sensors, integrated and stand-alone networks, and other systems. This can help identify patterns and anomalies that may indicate the presence of a multi-vector attack. This would assist in timely detection and identification of the multi-vector threat, thereby reducing the reaction time.
- **Operational Environment Analysis:** Data analysis, related to the operatinal environment and various scenarios to generate the likely CoA. For example, considering the present weather and threat parameters, real-time Intelligence, Surveillance and Reconnaissance (ISR). By analysing past data and current indicators, AI models can also forecast potential attacks,

anticipate adversary strategies and identify vulnerabilities before its exploitation

- **Objective Identification and Strategy Formulation:** AI can work out various combinations to match the strategic objectives with the user input, towards which the subsequent planning may be formulated.
- **Analysis of Operating Constraints:** This involves scrutiny of existing limitations of the system and its associated environment under which the operations would be undertaken. The analysis would aim at shortlisting the best solutions, with the current restraints and governing rules.
- **AI-Enhanced C2: Decision Support in the Selection of Most Appropriate CoA:** AI can provide decision-makers with critical information to base their decisions, including the likelihood of success, potential risks, and recommended courses of action.
- **Autonomous Response**: AI can automate responses to multiple types of attacks, reducing the response time and increasing the effectiveness of the response. The previous steps of selection of the best tactical action and its timely execution will govern this.

In essence, AI, if implemented efficiently, can act as a force multiplier and combat enabler for military entities. The integration of AI would allow the forces to operate with greater speed, precision and efficiency in complex and multi-vector threat scenarios. It would also enable automation of command and control against the traditional ways of the decision support system, which can easily be overwhelmed and made unusable by multi-domain attacks.

AI-Driven Command and Control (C2) Systems: Connecting the Dots with the Observe, Orient, Decide, Act (OODA) Loop

The concept of the AI-driven C2 concept refers to the integration of AI and algorithms into traditional command structures to

enhance decision-making speed, operational efficiency and overall effectiveness. As military operations by their very nature are complex, AI is emerging as a critical enabler and crucial component for decision-making and conflict resolution.

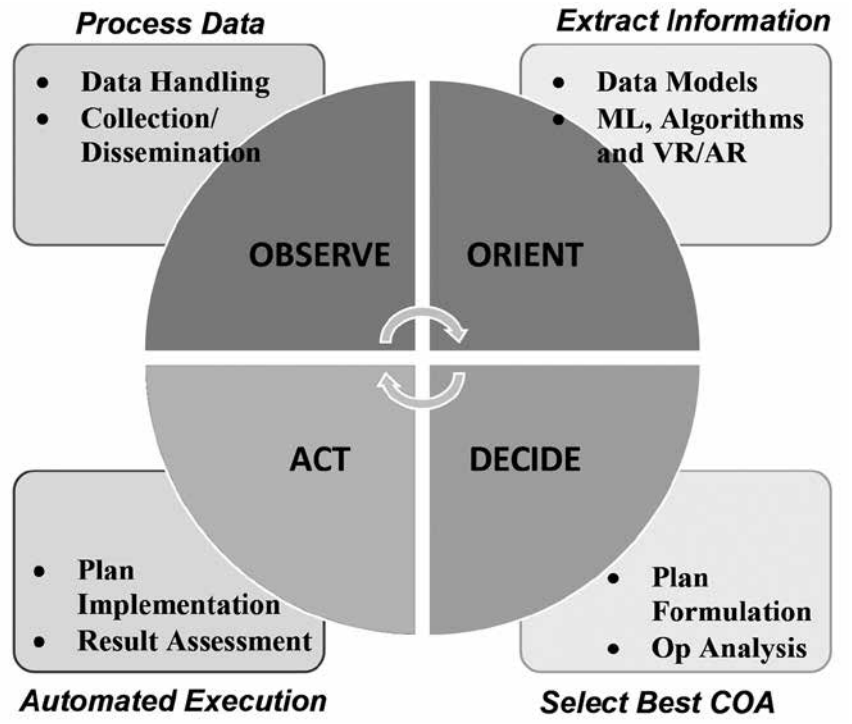
All military operators are aware on the significance of the OODA loop, as developed by United States Air Force (USAF) Colonel John Boyd, for application to the combat operations process, often at the operational level, during military campaigns.[5] As described by Harold H.M. Vermanen, one of the ways to apply the OODA concept in C2 is to get inside the attacker's loop and rapidly increase one's own chances of victory by taking the initiative before the attack takes place.[6] This effort will focus on defence by affecting the decision-making process of the adversary before the attack is launched.

The same principle of the OODA loop can be applied in the AI-driven C2 concept at all levels, thus, shortening the decision-making matrix, as most of the complexities would have been addressed by the pre-fed/refined algorithms at various verticals. Due to the system-enabled transparency; a proposed best CoA can now easily be referred back and forth by all the stakeholders, thus, simplifying decision-making and execution at the opportune time and place. Added to this, all the commanders would know the real-time availability of the given resources at their disposal as the AI grid will calculate the actual consumption, thus, forecasting the requirement for the ongoing and future operations. Every entity in an AI grid will now have been made aware of the rationale of reaching the most optimum tactical CoA.

5. *Science Strategy and War, The Strategic Theory of John Boyd* (Abingdon, UK: Routledge), ISBN 0-415-37103.
6. Harold H.M. Vermanen, "Command and Control in Digital Transformation: The Future of the Command Post", *NE Journal*, Edition 28 (Cyberspace Operations), December 2019.

Another way to implement the OODA loop in the C2 system is to redesign/realign/remodel the conventional means of warfare with the assistance of AI/ML to make them relevant in the current technological intensive warfare, which would necessitate utilising the processing edge of AI and ML in the mission planning process to arrive at the most potent, workable, tactical plans. A description of this is given in Fig 3.

Fig 3: Implementation of the OODA Loop in the AI-driven C2 System

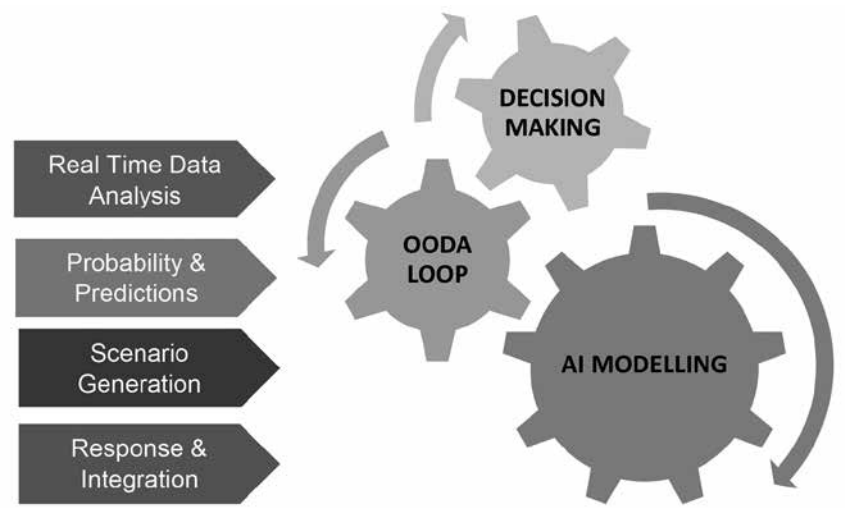


- **Observe**: This step involves processing of a mammoth amount of data, collected from varied sources and networks, which is beyond the usage capacity of conventional machines. AI assists in integrating the larger combat enablers to refine

the analysis process as per the given operational/tactical environment.

- **Orient**: Once sifting of the enormous quantity data is carried out, it will be subjected to pre-decided algorithms and data modelling to extract viable information. The models can further be refined with the help of ML and Virtual Reality/ Augmented Reality (VR/AR). This step will effectively guide the efforts of the C2 system towards the designated objectives.
- **Decide**: Post data processing and streamlining of actions, analysis of past data, previous results, recurring patterns and anomalies will be matched to find out the best CoA for the situation.
- **Act**: The OODA loop will be completed with the execution of the CoA. The response may be automated with minimum human intervention, utilising AI and ML.

Fig 4: Implementation of AI in the OODA Concept



Case Studies: AI Concepts Already in Use for Military Operations

There are several examples of AI that are being used in military operations to enhance command and control and respond to multi-vector attacks. Some examples include:

- **The IAF Integrated Command and Control System (IACCS):** The IACCS network integrates all sensors (civil/military) across all the Services (army/navy/air force) to provide a fused air situation picture to the commander. It further utilises the user's input with AI to generate automated solutions for efficient battle management and threat evaluation.
- **The US Department of Defence's (DoD's) Joint All-Domain Command and Control (JADC2) Programme**: This programme enables sharing of information across all domains (land, sea, air, space, and cyber) in real-time, using AI and ML to analyse and process data.
- **The UK Ministry of Defence's (MoD's) Autonomous Warrior Programme:** This programme is in use by the UK Army and it enables the commanders to provide support in decision-making on the battlefield by real-time detection of threats.
- **The Israeli Defence Forces' (IDF's) AI-Powered Command and Control System, Iron Dome**: This system uses AI to analyse data from various sources, including sensors, networks, and other systems, to identify potential threats and the best solution, and precisely destroy it with the best combination.

CHALLENGES AND LIMITATIONS

While AI has the potential to revolutionise command and control in military operations, enabling rapid response to multi-vector attacks and enhancing the effectiveness of military operations, there are several challenges and limitations, which must be addressed.

- **Data Dependence**: The AI system is one of the systems to process the inputs of numerous systems, thus, the outcome is input dependent. Hence, the quality of the data used as reference is critical and sub-optimal data can produce non-workable decisions/outcome.
- **Authenticity:** Ascertaining the legitimacy of solutions delivered by the AI system will remain a critical factor. At times, the authenticity of the delivered information may be corrupted by over-amplification. Assignment of negative values to bad data entry and enabling transparency, with the required human intervention, will provide a logical approach to commanders.
- **Interoperability**: The ability of different systems to share information and work together seamlessly is critical, and interoperability can be a challenge while applying AI-driven C2 in integrated networks and domains.
- **Information Security:** The use of AI in the C2 systems can create new cyber security risks such as the potential for AI systems to be compromised or manipulated.

CONCLUSION

While challenges related to data quality, trust and information security remain, the benefits of AI-driven C2 are far too many. By focussing on human-AI collaboration and ethical innovation, the defence sector can unlock the full potential of the AI-driven decision support system, ensuring effective and responsible command in the complex operational environments of the future.[7] By leveraging the power of AI, military organisations can gain a strategic advantage, stay ahead of emerging threats, and protect their forces and assets.

7. "The Future of Command: AI-Driven Decision Support System in Defence", Defense Innovation, Brite Innovation Review.

The future comes faster than we can even imagine. The outcome of any futuristic battle will depend on the best AI technology and its judicious use by the most sane and logical man behind that technology. In conclusion, quoting the perspective of Microsoft Chief Executive Officer (CEO) Satya Nadella on how AI should evolve: "We need to take accountability for the AI we create. With any new technology, we as a society, have to be clear-eyed on both sides of it—the opportunities for this technology to have a profound impact on our daily lives and do good, and, at the same time, be very mindful of unintended consequences." Militaries worldwide are adapting to the AI, ML process and keeping pace with this is a necessity to maintain the operational edge in all spectrum of warfare. The sooner, the better.