



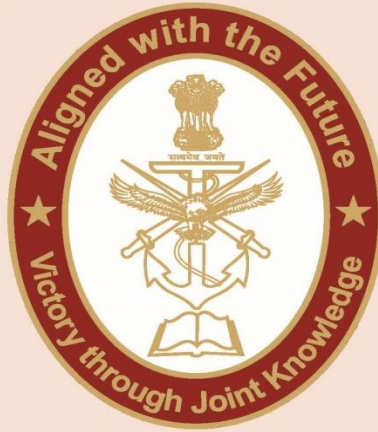
CENJOWS

WEB ARTICLE
WA/35/24

AI FOR EFFICIENT UTILISATION OF ISR IN JOINT OPS: CHALLENGES AND RESOLUTIONS

GP CAPT KANCHERLA ARUN KUMAR

CENTRE FOR JOINT WARFARE STUDIES



CENJOWS

AI FOR EFFICIENT UTILISATION OF ISR IN JOINT OPS: CHALLENGES AND RESOLUTIONS



Gp Capt Kancherla Arun Kumar, is a commissioned officer in the Aeronautical Engineering branch of IAF.

Introduction

The recent conflicts like the Russia-Ukraine war or the Israel-Hamas conflict have busted the myth of short conflicts and have highlighted the importance of availability of Intelligence. Tactics and Technology go hand in hand to protect own interests and defeat the adversary. They complement each other to ensure success. Tactics work when technology is employed in the right perspective and in an innovative manner. Employment of drones, camouflage of tanks in cost of effective manner, indicates tactics using technology. Another aspect that is highlighted is the need for joint ops to ensure total control of the situation.

Success of Joint Ops depends on synergy between the stakeholders involved.¹ Sharing of “Information” and “Intelligence” is paramount for effective operations. Sharing of information or intelligence is not only critical for success of joint ops but also to avoid fratricide and reduction in economy of effort. Shared Situational Awareness (SSA) facilitates effective ops with least damage to own forces. Over a period of time, owing to advent of technology, the concepts have graduated from C2 i.e. Command & Control to C6ISR, Communication, Computers, Cyber-defense and Combat Systems

being the 3rd, 4th, 5th and 6th Cs. However, C2 continue to be the focus of success in any situation. The other Cs are just the “means” assisting the Commanders, through Command & Control, in achieving the “ends”. A weak C2 can never ensure success irrespective of the capability being enhanced through the other Cs. In other words, a formidable C2 is the fountainhead of success in any conflict. Availability of “Credible” and “Actionable” intelligence is critical for commanders to plan and execute operations.

Relevance of ISR in Joint Ops

Commanders have to operate at different levels depending on the state of War / Conflict, namely, during peace, no war no peace and limited offensive ops / conflicts / war etc. Depending on the state the intelligence requirements would also be classified as Strategic and Tactical. Strategic intelligence assists long term planning and strategy formulation, while the tactical intelligence is critical in terms of “currency” and “validity” of the information for “Time Sensitive Action / targeting”.

Thus, ISR holds high relevance in ensuring availability of Credible and Actionable intelligence to the commanders. ISR is a vast and diverse field with different types of sensors which consists of different types of SIGINT sensors (ELINT & COMINT) employed from different geographical features. We have Ground to Air, Air to Air, Air to Ground, Ground to Ground and Space based assets for INT gathering. RADARS including SAR/ISAR sensors, EO/IR sensors, and COMINT sensors comprise the large modes of INT gathering. We should not forget another important source of information i.e. the Cyber Source. This information needs to be further corroborated with the other intelligence gathering methods i.e. HUMINT and OSINT in order to establish the validity and importance of the available information.

Each arm of service over a period of time has developed its own set of ISR assets. Access to the information and intelligence gathered through these sources is shared with other arms depending on requirements. However, joint access, sharing and seamless integration of these sources is necessary to facilitate effective collaborative decision making in joint ops. A good glimpse of success of such collaboration was on display during the operation desert storm by the allied forces.

However, the diverse types of sensors contribute to enormous volume of data in different formats, e.g. ELINT Data including Emitter Signatures, SAR images, EOIR images and COMINT Data etc. Co-relating the information received through each type of sensor is a challenging activity needing acute knowledge and analyzing skills.

“Artificial Intelligence” (AI) and “Machine Learning” (ML) are being projected as panacea to tackle all such problems. AI is expected to provide quick solutions to the commanders, both at Strategic and Tactical levels, to guarantee success in operations. Not surprisingly, AI employment is expected to assist the commanders in faster analysis of data and provide “intelligent” inputs.

The world today is talking about **Intelligence Enabled Warfare (IEW)** wherein Command & Control is exercised through two forms of intelligence i.e. Humans & Machines thus giving rise to the term C2I2 framework. Contested environments present some challenges like connectivity between different resources and this has led to the idea of developing AI enabled tactical systems that connect at will with reduced EMS footprints. These kinds of systems are expected to facilitate collaborative ISR by “autonomous” systems. Therefore, the expected end result is to have “autonomous” weapons systems that are capable of taking “decisions”. These systems are expected to effectively “**reduce fog of war**”, increase synergy among the joint forces thus leading better coordinated operations, clarity in actions, better and reduced timing, effective time sensitive targeting and reduce chances of fratricide.

Challenges

Revolutionary advent in computing technology, enhanced research in quantum computing, increased development activities in the field of ML & AI have garnered lot of interest from the Defense industry. The aim is to leverage the advantage of this new age technology to enhance the capability / potency of the weapon systems while reducing risk to own forces. Employing this technology in ISR is expected to provide more accurate and credible information regarding the adversary for planning and executing precision attacks on centers of gravity.

Though all this appears to be very tempting, the whole idea and exercise comes with its own set of challenges. This paper aims to discuss a few of these challenges.

- (a) Each arm of the armed forces has inventory of different types of ISR sensors of different vintage and different sources (indigenous and imported). The Vintage and diverse Sources provide data in different formats and different volumes. Sensors providing information in similar format different in terms of some critical parameters like resolutions, coverage etc. Further, most of the OEMs ensure that their products are processed in proprietary formats which are not generally shared with the customers for obvious reasons. Thus, correlating the data from sensors of different vintage, different data formats and different types is a humongous challenge.
- (b) Another challenge, is correlation of data in Time Domain. Depending on the type of sensor, data from different sensors is captured in different time lines. Similarly, Data, of same area / object, would be collected by different sensors from different positions and angles. Correlation and analysis of this kind of data not only requires high processing / computing capabilities but also communication channels having high data rate and ranges. These aspects become all the more critical when there is a need for real time information necessary for time sensitive action in a tactical situation.
- (c) Each type of sensor has specific strengths in providing “information”, correlation of information received from different types of sensors is necessary in creation of credible, verified and accurate “scenario” of the area of interest. But, as discussed correlation of data in different formats requires very advanced and matured “Systems”. This is possible only through availability of huge amounts of data over a long period to assist adequate training of the systems. Further, it is necessary to ensure that the data being fed to these “Systems” is purified and rationalized. Data purification is necessary to remove the biases introduced due to the difference in “capabilities” of the source sensors. Therefore, interoperability, standardization and backward compatibility are going to be the major challenges requiring special focus.
- (d) As discussed above, comparing and co-relating data within a single arm in itself is challenging. The situation becomes all the more complex as each fighting arm interprets and analyzes the data in a specific way that suits its concept and style of operations. The perspective of army would be altogether different from that of Air Force or Navy or any other agency participating in the operations. In joint operations there would be a requirement of interpreting available data in a joint

perspective with capability to present the same information in the right perspective to each participant.

- (e) Expediency of information and intelligence gathered during peace is one of the major areas of concerns. It is but prudent to expect that the adversary would not be positioning the formations at the same locations during operations / conflicts. Everything from locations to signal characteristics would be changing during engagement. Therefore, the data used to train an AI System would predominantly consist of data collected during peace time. One of the major requirements during operations is “correct identification and classification” of the target which depends on different intelligence inputs. Thus, in a real conflict the data collated over a period of time, in peace, might not be of much help in “identification and classification” by the systems which have been trained using volumes of data collected during peace. If not trained properly, during joint ops, the system might unwittingly assist in fratricide. This kind of situation shifts focus towards capability of the decision support systems to “identify and classify” correctly in absence of adequate data.

Way Ahead & Resolution

Synergy during joint ops cannot be assured just by use of AI. Concerted and sustained joint exercises are bare minimum requirements in order to streamline the concepts and induce synergy among different arms. The purpose of the joint exercises / war games is to first streamline joint op concepts while exploring the strategies and concepts expected to be employed by the adversary. The efforts should try to find solutions to the challenges discussed earlier in this paper. Some of the actions that are mandatory towards achieving synergy are discussed in subsequent paragraphs.

- (a) Development of a framework that facilitates integration of all the sensors and sources of intelligence that would ensure capability enhancement. Success cannot be guaranteed if agencies work in silos. Synergy within and between agencies is mandatory, therefore, the framework being developed needs to be designed in such a manner that there is seamless integration of assets.

There are many studies and research projects that have professed use of AI to overcome the challenges posed due variety of sensors available in the ISR field.

These solutions predominantly provide solutions for fusion of data sets available in different formats, Secure communication networks that could facilitate interoperability in denied or contested environments etc. This would facilitate better coordination during joint ops. However, the utilization of these concepts would be possible only through a joint effort through an apex body that would control and manage the integration of ISR assets.

- (b) Many would argue that Standardizing formats would ease the process of correlation and integration. Though technically it would be right but prudence says that it would compromise the systems and make them more vulnerable. The challenge is to develop frameworks and systems that are capable of integrating systems of different types, specifications and formats. It is to be remembered that it is difficult but not impossible. It goes without saying that absolute accuracy can never be achieved. Every system is bound to have its own biases and additional biases are likely to be introduced during the integration. Though, proper design may help the system in negating individual biases.
- (c) Regular joint operations, simulating, realistic op situations in order to generate enough data for training the AI Systems over a period of time. It is not to be forgotten that the AI Systems would mature over a period of time only with increase in purified and realistic data. It should be ensured that “false” results are not allowed to creep into the system. Camaraderie and joint concepts of operation are cornerstones for generating realistic data for AI systems.
- (d) Collaboration from the very beginning would be a good way to reduce the complexities that could be anticipated in integration of systems from different agencies. Joint committee should be formed to plan and execute the programme.
- (e) It is not to be forgotten that there is a need to recognize and leverage the advances made in the civil society in field of AI. AI is being explored right from Supply Chain management, SCADA management, manufacturing and production, Cinematics & Video gaming to medical field in the civil world. There is a scope to imbibe and tweak the technology for military use. Therefore, the participation of industry and academia in the joint committee would enhance the effectiveness of the committee.

- (f) “Environment” – The Information environment is described to be consisting of three dimensions, namely the physical, cognitive, and informational processing.² The physical and cognitive dimensions are the complex parts and pose the actual challenges. Therefore, there is a need to address these aspects while training the systems.

Human Factor affecting AI enabled systems

Autonomous weapon systems have been in discussion for some time now. AI is expected to substitute human beings at many places thus reducing risk to troops while increasing damage to the adversary. Autonomy may give some advantages however, there are some drawbacks owing to need for adequate maturity of systems. Ample study is available on maturity of autonomous systems, legal issues and ethics in using the lethal autonomous systems.³ AI powered decision support systems induce some drawbacks that would undermine human capabilities over a period of time.

History is witness to the fact that dependence on technology has reduced human capabilities / faculties. A simple example is what we see today in terms of simple mathematical calculations, the younger generation is getting used to using calculators. Counter argument would be that technology helps in saving time. However, one needs to understand the difference in usage of technology for civil purpose and military purpose. The battlefield is unpredictable and technology is always susceptible to disruption through usage of superior technology or human intervention. Human ingenuity, unpredictability of human thought and radical decisions by field commanders can change the course of operations in most adverse situations.⁴ Overdependence on decision support systems, powered by AI and ML, are likely to weaken these faculties of human brain and thus dilute the quality of commanders in future.⁵ Under pressure the commanders might be tempted to stick to “suggestions” of such systems rather than analyzing the situation on their own or trusting their “instincts”. These would definitely compromise the operations. War Games and exercises simulate situations where the field commanders exercise their cerebral faculties in decision making. The outcome these war games and exercises would ultimately be part of the data used for training of AI powered systems.

Another important human factor in development of AI powers systems is Trainer Capability. Every human, irrespective of training status, is bound to have internal biases due different situations faced by him / her.⁶ This in turn would convert into “training Biases” depending on the personal characteristics of the trainer. Therefore, there are very good chances that though the data analysis is at a faster pace, however, the resultant solutions would not necessarily be perfect or free of errors. The solutions are likely to have similar success rates. This is where the Human intelligence and “prudence” comes into picture. *Experience, Common Sense and Wisdom* are unique characteristics of each Commander. *Intelligence Quotient and Emotional Quotient* of a Commander are critical characteristics that determine the “prudence” of the decision taken under stress or duress. No amount of war games or exercise would be able to generate the kind of stress or duress that would be experienced during a real situation. Real situations would evoke the best instincts and faculties in a commander which can never be replaced by a machine. At the most, AI solution would be an amalgamation of the collective characteristics of different trainers.

An example of collaborative ISR system

Though many countries have been working on integration of intelligence from different sources, US has been a front runner in integrating the information and converting the process into a potent “weapon system”. The system has a layered framework in form of Distributed Common Ground System (DCGS) for Army, Navy, Air Force and the Marine Corps.⁷ This is further integrated into a common system, namely, DCGS-I (Distributed Common Ground Stations - Integrated). The “weapon system” has been developed over a period of time and is being utilized by the US authorities. This system is an excellent example of synergy and reflects optimization through integration of intelligence gathered by various agencies including the Armed forces and Home land security agencies. Apart from the security agencies, this system also facilitates integration of other public utility systems like the traffic management system, telecom services etc. to gather information and use the information in identifying the threat. However, it goes without saying that even these kinds of systems assist the decision makers in hastening the process of taking decisions.

Areas for further Studies

There many other aspects that have not been discussed here. One of the major aspects is the security aspect. Like all technologies AI too has a dark side that needs adequate consideration while exploring usage and dependence on AI for critical activities like war fighting. Enough evidence is available about misuse of AI in form of deep fakes etc. AI systems that are engaged for IEW therefore need to have stringent security features. Even with having stringent security features the threat of “misguiding” or training the system with malicious intents cannot be ignored. These factors open a wide area of study in order to strengthen the AI-Enabled systems.

Conclusion

Integration of assets to leverage the existing ISR sensors of all the agencies would enhance capabilities during joint operations. More credible information can be presented in the right perspective to enhance effectiveness of the joint ops. However, we need to remember that Machines have limitations. They can at the most help humans in taking a measured decision. However, humans are gifted with something known as “Common Sense” and “Wisdom”. Wisdom comes with experience and helps in “Out of Box” thinking which is necessary to win a conflict / war against a worthy adversary. “Artificial” will never be able to match the unfathomable power of human brain. Artificial Intelligence can act as a Decision Support System but cannot replace the Human factor in the loop. Too much dependence on technology could lead to a situation where in the future generations are not willing to use the “natural” faculties and thus become “Slaves” to their own creation i.e. the “Machine”.

Hence, there is a need to identify the area and the extent to which one would like to employ technology. AI provides a range of opportunities in integration of ISR sensors, data crunching, milking of “actionable” information and dissemination to the soldier in field in limited time domain. It effectively contributes to reduction of time for dissemination of “information and intelligence” in the OODA loop. If harnessed properly, AI tools and AI systems would act as effective “decision support systems” to help the commanders in taking “measured” decisions.

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 Joint Publication 5-0, Joint Operation Planning (Washington, DC: Joint Chiefs of Staff, August 11, 2011)

² Joint Publication 3-13, Information Operations (Washington, DC: Joint Chiefs of Staff, November 27, 2012), I-2

³ Shayne Longpre, Rishi Shah et. al; "Lethal autonomous weapons systems & artificial intelligence: Trends, Challenges, and policies" (MIT Sciency Policy Review, Vol 3, pp 47-56, August 29, 2022)

⁴ Frank Hoffman and Michael C. Davies; "Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?" (Small Wars Journal, Jun 10 2013)

⁵ Vicente, L., Matute, H. Humans inherit artificial intelligence biases. *Sci Rep* 13, 15737 (2023). <https://doi.org/10.1038/s41598-023-42384-8>

⁶ Marinucci, L., Mazzuca, C. & Gangemi, A. Exposing implicit biases and stereotypes in human and artificial intelligence: state of the art and challenges with a focus on gender. *AI & Soc* 38, 747–761 (2023). <https://doi.org/10.1007/s00146-022-01474-3>

⁷ Lt Col Jason M. Brown, "Operating the Distributed Common Ground System: A look at the Human Factor in Net-Centric Operations" (Air & Space Power Journal, Winter 2009, pp 51-57)

Bibliography

1. Steven Rogers, Jared Culbertson et. al; "The QuEST for multi-sensor big data ISR situation understanding" (Ground / Air Multisensor interoperability, Integration and Networking for Persistent ISR VII, Proc. Of SPIE Vol. 9831, 2016 SPIE)
2. Sean A. Atkins; "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace" (Air & Space Power Journal (Vol. 32, Issue 3), Air University Press, Fall 2018, pp. 26+)
3. Haase, Eugene. "Distributed Common Ground System-Future." *JFQ* (2015): 109-113.
4. Peter Layton; "Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars", (Joint Studies Paper Series No. 4, Australian Defence College Publications, 2021)
5. Sungrim Cho, Woochang Shin et al.; "Priority Determination to Apply Artificial Intelligence Technology in Military Intelligence Areas", *Electronics*, December 2020, 9, 2187; doi:10.3390/electronics9122187
6. J Z. Bakdash, D Pizzocaro & A Precee; "Human Factors in Intelligence, Surveillance, and Reconnaissance: Gaps for Soldiers and Technology Recommendations", IEEE Military Communications Conference, San Diego, CA, 18-20 November 2013.