

CENTRE FOR JOINT WARFARE STUDIES

# REPORT ON DELIBERATIONS GAISA 4.0

ORGANIZED BY CENJOWS & AICRA 18-19 JANUARY 2024

#### U. dialogin

ykanas rins ( lut ayd ki 38km, m k-nkama 48km lut a-c kama hog ; akdaagt yluus i alendd gyk;

#### 12473421+ kj ne od ayloina rn4, syloina rn5, ayloena rn ayloena rn7, ayloena rn8 ( signa : 52vd 2 42vd; vg i g m 2

32473428s kj ageriger n6 ( Tuttagel ki ortvali

) 32473428a ki ep



WWW.CENJOWS.IN



The Centre for Joint Warfare Studies (CENJOWS), in collaboration with All India Council for Robotics & Automation (AICRA), conducted a two-day seminar, "GLOBAL ARTIFICIAL INTELLIGENCE SUMMIT 4.0", from on January 18-19, 2024. The event was conducted at Manekshaw Centre, New Delhi. Eminent panellists in the conference were Senior Serving Officers from tri-services, scientists from DRDO, Academia and Industry. The seminar offered an environment for the industry to interact with the armed forces to understand AI requirements of the tri-services and offer solutions. The event was instrumental in generating awareness amongst the audience about the technical advancements achieved by the DRDO in the field of AI and robotics.

# Day 1: Inaugural Address

The GAISA 4.0 was inaugurated by **Admiral R Hari Kumar, PVSM, AVSM, ADC, Chief of Naval Staff**. He expressed his delight at being able to deliver the Keynote Address for the Fourth edition of GAISA and on the aspect of the themes selected for the Seminar viz Military Applications of AI & Robotics, Cyber Security, Health Care and Education. He commended the active participation of distinguished stakeholders representing various ministries and departments and highlighted that advancements in niche fields of AI and Autonomous Technologies could well shape the growth of Bharat in the Kartavya Kaal.

The CNS mentioned that we are witnessing "A vibrant AI Innovation Spirit" as articulated by the Honourable PM during Global Partnership on AI Summit. He expressed that we need to harness the spirit to propel our capability to the future and make Bharat a global leader on AI and related technology and seminars like this will be instrumental towards the same. The CNS highlighted the aspects of responsible and ethical use of AI and exhorted the industry and Forces to envision and encourage a future where AI is seamlessly integrated into our lives for enhancing efficiency, reducing risk, and offering optimum solutions to challenges that were once considered insurmountable.

The CNS covered the disproportionate role of AI during recent Russia-Ukraine and West Asia Conflicts to include unmanned systems, facial recognition for targeted attacks and ambiguity over information on TV screens.

The CNS underscored the crucial role of People (Human skill and Wisdom), Policies (Protect Systems, Networks and Data Privacy for Cyber Security and promote Indigenous Industry for AI tech) and Pole-Vaulting technologies (identify means to leapfrog existing tech curve and identify new frontiers to pole-vault to emerge as leaders in AI and robotics).



**Dr Sameer V Kamat**, Secretary Dept of Defence R&D & Chairman DRDO, delivered the keynote. He stressed that as technology advances; nations worldwide explore innovative ways to strengthen their security apparatus. Among the entire emerging tech, AI will play a critical role in the realm of military and national security. AI has the potential to revolutionise military capabilities, enhancing efficiency, accuracy and overall effectiveness. One of the primary advantages of AI in defence is its capacity to process vast amounts of data in the shortest possible time and at an incredible speed. This allows the military to analyse intel from various sources like satellite, drones and all other sensors in real time; the result is a more comprehensive and timely understanding of the battlefield enabling quicker decision making. AI is a tech which facilitates autonomous UAVs in surveillance and in assaults. It is also going to accelerate autonomous underwater vehicles and autonomous land vehicles, which is soon going to be a regular feature in warfare.

In addition to physical platforms, AI is a critical addition to the cyber domain. The defence sector is frequently under the threat of cyberattacks. AI defence systems can analyse to detect and counter these attacks in real time. As our warfare evolves, attempts will be made to disable the critical infra. Hence, we must develop AI tools to help us in cyber defence to win future wars. Collaboration between human and AI is pivotal in optimising defence capabilities. The synergy between human decision makers and AI systems creates a force multiplier effect which will enhance the overall military performance. Ethical considerations must also be taken into account. DRDO is also studying AI algorithms that can be embedded to increase the efficiency of military systems.

Air Vice Marshal Sanjay Bhatnagar, VM, VSM (Retd), officiating Director CENJOWS, proposed the Vote of Thanks by expressing his gratitude to Chief of Naval Staff, Admiral R Hari Kumar, Secretary DRDO, Air Marshal Anil Chopra (Retd), DG CAPS, Lt Gen Vinod G Khandare (Retd) and Mr Raj Kumar Verma, President AICRA. AVM Bhatnagar also thanked the encouraging participation by veterans, serving officers from Armed forces, CAPFs, industry and media and delegates from friendly foreign countries. He highlighted that one of the important charters of CENJOWS is free dialogue and discussion on issues that have a bearing on joint warfare and on formulation of policy options. CENJOWS has been holding seminars, forums and discussions on transformative and disruptive technologies at various junctures.

He stressed that AI is one such technology which impacts us all. AI, ML and robotics have great amount of employment in tri services and are important in unique ways to make better and timely decisions by commanders from battlefield to operation centres. It is finding ways into planning tools, decision support systems, collection and fusion of intelligence, surveillance and reconnaissance data for enhanced domain awareness in air, water and land. Manned Unmanned Teaming (MUM-T) and swarms are being



employed by all services. Al rides on robust VOIP communication network with redundancy and cybersecurity built in. This network is being converted into a tri services system. Employment of AI in every military application with support from academia, R&D organizations is need of the hour. Indian Army Indian, Air Force and Indian Navy have established AI centres of excellence and innovations hub in various parts of the country with required investments. These centres are developing various programs with the help of industry.

AVM Bhatnagar thanked AICRA for planning a full day discussions on AI applications in defence with focused deliberations on policy framework and applications of these techniques to make armed forces more potent. He mentioned that CENJOWS and AICRA would be taking up these proposals up the chain to seek the decisions required. These forums enable armed forces in a big way to synergize its efforts with industries thereby fostering military industry partnership in defence manufacturing. In the end, AVM Bhatnagar expressed his gratitude to HQ IDS for the continued support rendered and Team CENJOWS for organizing the event.

# SESSION 1: GLOBAL TRENDS IN MILITARY ROBOTICS & AUTONOMOUS SYSTEMS AND KEY TAKEAWAYS

### Key Takeaways from the talk by Ms. Desiraju Padma, Scientist G, CAIR, DRDO

- There have been numerous technological developments in recent years. The effective utilisation of autonomous vehicles, particularly drones, for precision attacks and even neutralisation of anti-national elements in civilian areas, a concept that was previously unconsidered due to the minimal collateral damage associated with such attacks, has been demonstrated in the two ongoing wars.
- An abundance of such applications is emerging, nearly altering the military paradigm. There are numerous discussions regarding the integration of automated weapons and vehicles into our defence systems. For instance, the introduction of autonomous soldiers will undoubtedly raise new concerns regarding the testing and adoption of such equipment

# Key Takeaways from the talk by Gp Capt Sameer Joshi, CEO NewSpace Research & Technologies Pvt Ltd

- The military will prioritise the most optimal and tailored iterations of these types of advancements. This is the juncture where trust and ethics intersect, as clusters of these machines coalesce. Furthermore, they generate effects that will be of the utmost importance for military applications.
- When they collaborate with humans in the context of MUM-T, this is referred to as "manned unmanned teaming." As of 2030, the future combatants are the machines. With the assistance of artificial intelligence, autonomous robots



effectively will expand the military's presence into a fortified combat area by achieving greater range and persistence on the battlefield.

- It virtually guarantees extremely perilous and lethal missions, permitting more audacious concept operations. They both enhance surface and threat levels, as well as facilitate rapid penetration into heavily defended airspace, when combined. A firmly established paradigm of autonomous swarms will have developed by 2025, which will be highly critical and integrated with humanmachine and man-in-man teamwork.
- Cooperative Autonomy provides a contested battle space of the future, wherein distributed competition and computing in a distributed deviation coexist. Similar to unmanned wingman and permission flight, flocking involves the collaboration of specific robots, one in a primary role and the other in a robotic role. Once more, this is substantially regulated by algorithms. Swarming is entirely regulated by algorithms with human oversight.
- Over time, mass martial combat has comprised the majority of the evolution of warfare. However, when many of them combined, they were capable of producing a multitude of effects. However, it was subsequently halted in its tracks by a phenomenon known as the generation of mass. This contributed in some way to the widespread availability of manoeuvrable water. This began, you know, after the introduction of tanks and other IFVs during World War I.
- On the battlefield, COTS-based customised robotics, autonomous air, and mesh network advancements are largely observed. Effective communication becomes a critical attribute when a considerable number of agents are required to collaborate. Clearly, the motivations are that if we can generate mass over a specific area with these autonomous agents, that mass will assist us in producing the saturation effect that everyone desires. Obviously, this mechanised mass would then function considerably more efficiently in hostile environments and treacherous terrains. Clearly, human beings possess a certain degree of limitation.
- Diverse requirements and weaponry are involved; the larger objective and distribution are determined by the human, but the manner in which the mission is executed—including surveillance, logistics drops, and kinetic strikes—is determined by these agents who are receiving emerging intelligence.
- Presently, these unmanned agents possess the capacity for collaboration and autonomy when they operate in concert, under substantial human oversight. The role of the combatant may be transitioned from one of control to one of command. At this juncture, collaborative autonomy emerges as an advantageous form of autonomy. Additionally, a multitude of cooperative operations are feasible.
- MUM-T essentially amalgamates the capabilities of piloted platforms augmented by unmanned units in order to enhance situational awareness,



mission efficacy, and SA. As indicated by the result, it may grant you the ability to conduct ISR and kinetic combat support missions in contested airspace.

- Attacks have been launched against Saudi Arabia and all other nations; this serves as a single example of the events that are currently transpiring. There have been collaborative robot operations; the UAE is cooperating in Nagorno, Karabakh, Syria, and the current situation in Ukraine.
- Those who figure out the most effective ways to utilise this technology will emerge victorious in the robotic revolution, rather than those who develop it first or possess the most advanced technology. This is a notion that I believe is highly pertinent to the current era and environment.

# Key Takeaways from the talk by Maj Gen CS Maan, ADG-Army Design Bureau

- Four nations, albeit three in reality, due to the absence of publicly available information regarding the United States' military implementation of autonomous and robotic systems. China is concerned that their modernization consisted of three distinct phases or components: mechanisation, informationization, and intelligentization, which operates in the cognitive domain. China is considering the possibility that swarms will gradually supplant tactical levels of warfare, which are akin to the final line of defence.
- The UK—By integrating robotics and autonomous systems into human machine teams in order to generate mass and cadence while reducing risk, their overarching objective is to generate operational advantage for land forces. In fact, they desire for it to be forward-thinking, pertinent, and at the forefront of technological advancement. To put it broadly, mission support systems and operational areas comprise the two categories.
- Australia: Through RAS, they intend to establish and maintain competitive advantages for future land forces in accordance with their strategic vision. Optimising the efficacy of the combatant. The second is increased load carrying capacity, which could be achieved, for example, through the use of exoskeletons or other alternative load carrying options that can be put to use for carrying ammunition, goggles, visors for helmet-mounted displays; essentially, this would raise every soldier's awareness of the local area.
- Military deception can generate an array of distinct signatures while simultaneously amassing intelligence on the adversary. Efficiency and logistic awareness through the utilisation of sensors for predictive logistics, allowing the logistics component to be moved accordingly at any given time and location. Subsequently, predictive medical logistics is implemented through the use of ubiquitous sensors that monitor an individual's health status in conjunction with other integrated systems, which are once more supplied with the assistance of robotics.



- Ultimately, technology is only beneficial when it is incorporated into our operational philosophy and utilised accordingly. Thus, the armed forces face their true challenge in this regard, and they are striving to ensure that their operational employment philosophies can effectively leverage the potential of the RAS.
- Historically, the military has also considered the adversary, which may involve increasing investments in electronic warfare (EW) systems concurrently. However, in the end, everything is dependent on that, and doing so could render these systems ineffective or, at the very least, diminish their efficacy. EW while simultaneously implementing the most stringent measures feasible to reduce their signature. Consequently, covert measures are critical for all of our systems, including those that we develop using drones, clusters of drones, or any other type of drone.

# Key Takeaways the talk by Jigar Halani, Director - Solution Architect & Eng. at NVIDIA

- ChatGPT has significantly altered the prevailing terrain. In general, when we discuss AI, we refer to data, model training, biases and weights, and then the efficient deployment of the model. As soon as we incorporate the intricacies of construction and simulation, the stratum undergoes an increase in the quantity of components under consideration.
- In the past year, conventional route optimisation as it was performed by Uber and Ola has undergone a complete transformation, as has the application of the same algorithm by drones and robotics.

# Recommendations

India's future in AI and robotics can be shaped by several key suggestions. Significant resources should be allocated to research and development in these areas, fostering collaboration among academic, industrial, and government agencies. Ethical and regulatory frameworks should be established to ensure the development and deployment of AI and robotics technologies are governed by robust standards. Investing in educational programs and skill development initiatives is crucial for cultivating a diverse technology workforce. Prioritizing mission-critical applications in sectors like defence, healthcare, agriculture, disaster management, and healthcare can help tackle societal issues and strengthen national security. Infrastructure and ecosystem support should be established to support AI and robotics technology deployment. International collaboration should be encouraged to promote interoperability and global expertise. Lastly, indigenous AI and robotics solutions should be developed to address regional issues and enhance economic growth.



# ROUND TABLE MEETING 1: POLICIES AND ECOSYSTEM FOR ACCELERATED DEVELOPMENT AND INDUCTION OF AI & ROBOTICS ENABLED MILITARY SYSTEMS

### Chair: Dr N Ranjana, Director DSTA, DRDO

### Chairperson's Remarks

Industry can afford to go in a faster pace because the security and safety is not as much of an issue but that's not the case with the military. For development of military systems, there is a need of the military data to train the models and make this data sensible for the models then continuously adopt and stay relevant. The question of government versus private and strategy for de-duplication or a conscious duplication and a complementarity of the effort between the various segments or arms which are the stakeholders of this entire ecosystem. Software is a great asset but we need to also focus on hardware with the semiconductor machine. Lot of things are coming in but security of hardware and availability also needs to be a part of the policy development.

### Key Takeaways the talk by Dr Sarabjit Kaur, Scientist G (AI), DRDO

- Third party agency or a certification agency is a system to get trustworthy AI. Development practices should be followed properly so that there are no vulnerabilities and malicious functioning in the system. India, especially in defence, according to a document released by Department of Defence Production in 2022, 75 AI products of different categories were inducted in the defence
- Al is extremely powerful technology, but Al also brings new risks which are yet to be addressed. It has to be transparent, explainable, fair and impartial with safety and security issues. Al learns from data and data has biases, data has issues with its quantity and quality. Due to quantity and quality, the robustness is affected. Due to biases in the data, the fairness characteristic is affected. Of course, safety and security issues are there and with data also the privacy issues are there and it has a full development cycle.
- The European Union is the leader in developing strategies for trustworthy Al and AI regulatory frameworks. Throughout the world people are following European Union strategies. The EU has given ethics guidelines for trustworthy AI. They have proposed the AI Act in 2021, passed in parliament in December 2023 and it will be implemented from this year. Singapore also has very good trustworthy AI governance. They have a model AI governance framework which was published in 2019 and then the second volume was published in 2020.
- Indian government made the national strategy for AI, AI for all in 2018. It does not tall anything about trustworthy AI. In 2021, our government also came up



with the approach paper which defines all the characteristics of trustworthy and responsible AI. As far as trustworthy or responsible AI is concerned in India and we have a long roadmap to achieve in defence.

- The EU AI Act which is the first of its kind is going to be the first comprehensive law for the AI industry. It categorizes the AI applications according to the risk. There are four categories, minimal risk, limited risk, high risk and unacceptable risk application.
- US has a different approach. There are no regulations as such, but a blueprint for an AI Bill of Rights, which also talks about all these characteristics, safe, effective, algorithmic, discrimination, should not be there, data privacy, explanation and human alternatives should be there. NIST has come up with artificial intelligence risk-frame, risk management framework.US government has taken voluntary commitment from all top 15 companies to move towards safe, secure, and transparent development of AI companies include Amazon, Google, Meta, Microsoft, Open AI, Adobe.
- China has come up with big regulations, especially for the Generative AI and the regulation in August 2023. Security assessment has to be conducted before making services publicly available in accordance with the provisions. The responsibility lies with CAC- Cyberspace Administration Committee of China for the trustworthy part of AI.
- Open AI says that third-party auditing has to be there, red team exercises, bias and safety bounty programs and sharing of AI incidents have to be there.
- India is also in line with that By-2025, we should be also able to do first certification. India has to have a trustworthy AI framework developed, where we have to categorize the AI use cases based on their risk assessment and regulating them accordingly. The role of human intervention has to be defined according to the risk categorization.

# **Recommendation by the Speaker**

- The framework should be generic, sector agnostic, technology agnostic, algorithm agnostic, business model agnostic. It should be practical and implementable, and it has to be enforced by a regulatory body.
- Matrices and tests for checking trustworthy part of the AI. Researchers and industries have to make the principles and best practices to mitigate the harms of AI. User agencies have to demand trustworthy AI products. Organizations have to voluntarily abide with trustworthy AI principles and academic and training institutes have to conduct training programs for AI professionals.

# Key Takeaways from the talk Dr. Ashed Jamal, Scientist G - CAIR Bangalore

• Al is interested in annotated data. The domain knowledge is extremely important which is lacking is the annotated data. Annotation of the relevant



object category is necessary otherwise it will be a shallow model. There are more than 50-60 categories of different ships and the objects which are present in the sea in Navy and most of the people who are in DRDO or in industry will not be able to discriminate between different kinds of warships. Similar situation with anomaly detection in war regions.

- Al readiness is basically incubation of data, erudition of data, training of manpower, identification of people, or organization of the departments which is basically looking into adoption of Al.
- People normally upload their best quality images. Whereas in defence application, we deal with the worst quality images, worst quality scenario, worst quality situations. Therefore, we need to have a lot of emphasis on the realistic simulation of the environment, of the scenarios.

# SESSION2: LEVERAGING ARTIFICIAL INTELLIGENCE AND ROBOTICS FOR USE OF FORCE

# Chair: Air Marshal Ashutosh Dixit, AVSM, VM, VSM, DCAS, IAF.

# Chairperson's Remarks

The chair of the second session, opened the session by stating the relevance of robotics and automation in the military domain. According to the chair, the synergy and integration of artificial intelligence (AI) into tri-services fires are vital for an operational strategy that aims to achieve battlefield dominance and prompt response to the changing environment.

# Key Takeaways from the talk by Air Commodore Ashish Bhatia VM, Air Commodore Operations (Weapons), Air HQ

The speaker commenced his presentation by stating the importance of Collaborative Air Operations. The various vital arguments put forward were:

- The Indian Air Force (IAF) needs to field a credible force.
- Technology will define the connectivity between the conventional domains of land and air warfare systems.

The speaker emphasised the crucial nature of integrating manned and unmanned systems during the presentation, highlighting the SWARM Drones as an essential 'low-cost high-impact technology.'

- The importance of multi-use and multi-role drone systems was recognised due to their nature of providing multiple options to commanders on the battlefield.
- The integration of technology and military equipment demands the use of Al and secure communication as an absolute necessity.



Moreover, the innovative approach of Manned-Unmanned Training, also commonly known as MUM-T, was stated and defined as a 'force multiplier technology'. The approach also benefits the tri-services in the given ways:

- The system can perform high-risk missions on the battlefield with improved effectiveness and efficiency.
- It reduces the sensor to shooter time and benefits the ISR capabilities, protection, and deterrence.

During the closing remarks, the speaker emphasised the crucial need for the future of collaborative air operations through networking and combat aerial vehicles. He stressed the importance of building expertise and mastery through continuous testing and training and reducing and managing the human workload during manned or unmanned missions.

# Key takeaways from the talk by Commodore T Ajith Weapons & Electronic Systems Engineering Establishment, Indian Navy

The first point of the talk emphasised the crucial design criteria, with a strong focus on mission-specific adaptability, conventional and cyber security, and encrypted communication. The speaker elaborated on the requirement of making new AI-based automated systems keeping in mind the 'interoperability', i.e. technologies which are adaptable and usable with the present systems and human-machine interaction-based. The concept of integrating AI in aerial vehicles was discussed with a critical focus on:

- Data utilisation and sensor fusion for perception.
- Learning and adapting to evolving behaviour prediction for effective training and simulations.

The speaker further presented the 4 levels of automation in naval ships as the International Maritime Organisation prescribes. These are the Maritime Autonomous Surface Ships with varying degrees of automation as follows:

- Degree one: Ship with automated processes and decision support.
- Degree two: Remotely controlled ship with seafarers on board.
- Degree three: Remotely controlled ship without seafarers on board
- Degree four: Fully autonomous ship

The speaker concluded by presenting a roadmap for the Indian Navy. It included the integration of technology, critical capabilities, strategic efforts, and working of new and/or presently inducted systems of:

- Autonomous Surface Vehicle (ASV)
- Autonomous Unmanned Vehicle (AUV)



- Loitering Munitions
- Remotely piloted Automated Aerial Vehicles (AAV)
- AUV employed in INS Makar
- Automated Fast Intercept Boats (AFIB)
- Flare drones in surveillance
- Sea drones

# Key takeaways from the talk by Col Vivek Goyal, Colonel Strategic Planning, Tech & Al

The speaker began the presentation by taking instances from recent conflicts and establishing that this changing nature of warfare is driven by technology. Reiterating, he mentioned AI, an enabling technology, is most disruptive as it impacts physical, virtual and cognitive abilities. The US identifies AI as a key technology ensuring the country wins future wars. On the other hand, China describes AI as a critical strategic technology transiting from the concept of informational war to 'intelligentised warfare, aspiring to be an AI world leader by 2030 with a focus on Unmanned Combat Vehicle Systems. The speaker further highlighted potential areas for AI and robotics in the Indian Army, such as:

- Al brings cognitive capabilities to operational planning and decision-making to create a joint intelligence and operational picture.
- Al can enable the information and management systems for predictive analysis.
- The Army equipment weapon system and platforms can be enabled with AI, leading to enhanced robotics and uncrewed and unmanned autonomous systems in its inventory.

The automated lethal systems such as AI-based surveillance robots employed by both South Korea and Israel, China developing a Robotic Dog with a mounted rocket launcher, and Russia's Loiter Munition System were stated as benchmark examples. A robotic, unmanned and autonomous system has three categories of autonomy, which are:

- Human in the loop
- Human on the loop
- Human out of the loop

The speaker next highlighted the initiatives taken up by the Indian Army:

• In line with the Indian government's national strategy for AI, the Indian Army has its own policy document on leveraging AI and has evolved the AI Skill Roadmap for its personnel.



- The Indian Army has also laid down the policy of ethical and responsible AI, keeping in mind the transformative nature of AI and making it transparent and trusted.
- Army Training Command and Army Design Bureau provide numerous platforms with open challenges for synergising academia, industry partners and the Army.
- The Compendium of Problem Definition Statements 2023 indicates the Army's interests in AI-based unmanned teaming between tanks and drones, robotic mules, and tactical and technical training of mechanised forces.

The speaker concluded by stating the Indian Army's enormous canvas of operations with active borders where the employment ranges from full-scale to sub-conventional and is further complicated by the diverse, rugged and inhospitable terrain, which wears down both the technology and the machinery. The Indian Army's ambition of 2024 as the year of technological absorption and leveraging AI was made pivotal by the speaker for the army to become a future-ready, technology-driven, adaptive, responsive and resilient force.

# Key takeaways from the talk by Lt Col Aditya Bhosale, Military College of Electronics & Mechanical Engineering

The speaker's presentation focused solely on the land domain and the use of Unmanned Ground Vehicles (UGVs), commonly known as unmanned systems. The primary objective of UGV automation is to significantly augment human capacity in executing operations and groundwork, which were previously limiting factors. The levels of autonomy for these UGVs can be in the form of remote-controlled, remote-guided or totally autonomous systems. The aim of UGVs depends on various factors such as:

- <u>**Platforms</u>**: the terrains and place where the UGV is deployed, the time during which the operation is envisaged, and the size of the UGV to be employed in the operation.</u>
- **Sensors**: monitoring the pace, navigating data, collecting and processing it, and sending it back.
- <u>Control Systems</u>: The processing of data at the UGV level is a matter of concern where the control systems scheme out the data, process it, and predict the future course of action of that particular UGV.

The military application was showcased by citing the example of a soldier moving through an operation and having a situational awareness about the battlefield he is about to enter. The mission information of the adversity is obtained using surveillance and reconnaissance and/or using these UGVs. Among the examples presented were the DRDO-developed Daksh and Muntra-N UGVs, indigenously produced. Due to their



advanced capabilities and reliability, the Israel Guardium UGV and IDF's Jaguar UGV were also cited as essential examples. The speaker wrapped up their talk by highlighting the benefits of Unmanned Ground Vehicles (UGVs) as force multipliers. The integration of AI technology is set to give the Indian Army a significant advantage in terms of technology and operational effectiveness. The versatility and capability of each UGV is a crucial feature, with multi-domain applications currently undergoing extensive testing. There exists a necessity for 'human in the loop' and 'on the loop' for overall control of the automation.

# Key takeaways from the talk by Sandeep George, VP Technology –iMerit

During his presentation, the speaker began by asking the audience about the characteristics of good data. He then proceeded to explain that when data is collected from sensors and used in the AI field, it must go through a process of sifting through vast amounts of information to build the necessary capabilities to extract what is essential. The speaker emphasised the necessity of maintaining AI systems and launching products in an ever-changing environment. It is crucial that these systems can handle and adapt to the rapidly evolving needs of military scenarios, which often require reconfigured AI systems.

The automated military systems can be maintained by building effective AI data pipelines that can handle the underlying sensor information and scenario changes and adapt accordingly. The speaker introduced a novel concept of Generative AI that warrants serious consideration. He emphasised the significance of additional layers of security in the form of guard rails to be implemented by policymakers. This is due to the fact that the systems, relying on unsupervised data sets, are vulnerable to cyberattacks and corruption. The speaker emphasized the importance of collecting, curating, and monitoring data since the power of any AI system lies in the ability to extract relevant information from it.

### ROUND TABLE MEETING 2: CIVIL-MILITARY SYNERGY FOR HUMAN RESOURCE DEVELOPMENT TO LEVERAGE AI AND ROBOTICS FOR DEFENCE AND SECURITY

# Chair: Dr N Ranjana, Director DSTA, DRDO

### Chairperson's Remarks

The chair introduced the topic by stating the importance of civil-military synergy for human resource development, which is carried out by making experts in the country and through system efficiency.

She elaborated on the ethical dimension of AI and its implications for using automated systems and robotics by the tri-services. The chair emphasised the need to thoroughly



understand the moral considerations surrounding deploying AI-powered systems, particularly concerning national security matters.

The discussion shed light on the complex relationship between AI and ethics and the challenges of balancing technological progress with ethical concerns in military operations.

# Key takeaways from the talk by AVM Rajiva Ranjan, VM, ACAS Ops (Space) - Air HQ

The reality of warfare has significantly transformed in the post-Cold War era. The world has become increasingly unpredictable due to intense technological competition between established and emerging powers. It is evident that the military is struggling to keep up with the rapid advancements of Industry 4.0, a matter of great concern.

The recent conflicts have indicated a predominance and disruptive path of AI and operational and cognitive dominance.

The speaker also emphasised the importance of the man behind the machine. The shift from funds from military to civil expenditure was noted as a means of technological absorption.

The military has successfully implemented a range of cutting-edge initiatives, and by harnessing robotics and AI, the defence services are prepared to deter the adversary and add to innovation, economic growth, and national power. Some of the new initiatives are:

- ISR fusion
- Chain detection
- SWARM drones
- Logistical management
- Campaign planning and execution

The speaker gave an overview of China's developments in this field of technology:

- In 2021-22, the PLA inducted the concept of Multi-Domain Precision Warfare to leverage its C4ISR network, which incorporates big data and AI to rapidly identify adversaries' key vulnerabilities.
- The warfare technique helps their defence services maximise their gain and power by exploiting the civil-military fusion, coordinating technology innovation and the AI National Strategy.
- Most of China's AI projects are dual in nature and are driven by the PLA, emerging as an essential element of their Digital Silk Route.
- As part of this civil-military fusion, the number of private companies funding Albased military projects is increasing.



- The Chinese believe that the people and soldiers behind the machine are the sources of victory and that the soldier's mental and spiritual state is vital to winning the conflict. 13 Chinese universities and the famous 7 Suns of National Security of China, all centrally funded, provide human resources training for inducting these soldiers.
- The speaker mentioned the aggressive nature of seeking AI talent being carried out in China as part of their ambition to become an AI superpower by 2030, all for greater autonomy, ISR, and decision-making.

The speaker reiterated the significance of AI in national security and cited the Natarajan Chandrasekaran task force as an exemplary initiative by the Indian government to establish an institutional framework for integrating AI into national security.

He concluded his talk by highlighting the 'AI for AII' strategy with various centres, such as the Indian Navy Incubation Centre for AI (INICAI), and capacity-building by inducting defence personnel and veterans into such institutions. The round table discussion concluded with a lively discussion among the speakers and other panellists about the structure, command, and institutional framework for integrating the industries with the tri-services. The industrial perspective was contested, as was the role of academics and their insights into finding and placing talent.

# SESSION 3: AI AND ROBOTICS FOR CRITICAL MILITARY CAPABILITIES AND CYBER SECURITY.

The Session was chaired by Lt Gen MU Nair, PVSM, AVSM, SM (Retd), National Cyber Security Coordinator. He highlighted prevalent cyber security challenges in front of society as well for armed forces and how AI have started playing a crucial role in tackling this ever-increasing menace.

# Cmde Manish Anand: Defence Cyber Agency

- Speaker highlighted usage of AI from military perspective as well how Cyber Defence Agency is putting AI into use for Cyber defence in Military domain. He said that Cyber Defence Agency is a nodal Cyber Agency for defence forces which ensures cyber security of tri services cyber infrastructure against inimical threats.
- Capabilities of AI which are being exploited and major fields in which AI is being extensively used are Problem solving, perception/description, Natural learning processing pattern recognition, anomaly detection, behavioural analysis, classification etc.
- Further challenges being faced by defence forces in domain of cyber security such as large scale attacks, response beyond human scale processing



capability to detect/analyse were highlighted. Generative AI: Boon/Bane, malware development, manipulation of information, deep fakes, automated phishing etc.

- Traditional Defensive strategies against cybercrimes /threats have been outdated. Immediate requirement of more dynamic and proactive strategies is there wherein adequate user awareness should be a core component. Shortage of skilled manpower, expert in the field of cyber security is also being felt constantly.
- Damage to even highly secure military systems can't be ruled out in present day cyber conundrum. In spite of these systems being AV gapped IT/OT networks, shore based operational network, satellite communication network and other safeguard measures, these systems remain vulnerable to cyber threats.
- Threat to classified information always poses threat to military missions. Military systems being damaged /disabled at critical juncture may jeopardise military operations to an extent and endanger lives.
- Digital transformation of systems has led to many military actions/operations being transferred to internet further exposing military systems to cyber threats.
- High impact threats in the form of Insider threat, Supply Chain targeting, advanced persistent threat and social engineering do exist against military systems.
- Salient aspects of military systems which give them exclusivity are time critical, legacy systems, sensitive data, deep evaluation and capability to function without the internet.

# **Recommendations**

The Speaker highlighted following for security of defence cyber systems:-

- Need for AI/ML based advanced detection tools to include Security Operation Centre (SOC), Identify new types of Malware, maintaining competitiveness in field, NW/user behaviour analysis and predict potential attacks.
- Enhanced identification protection and authentication to include Facial recognition / CAPTCHA, Bot detection, Breach risk prediction, cognitive IW (deep fakes), secure code generation, threat limitation, reverse engineering and forensic education inclusive of password cracking etc.

# Wg Cdr Prateek Thapar: UDAAN, Indian Air Force

• Speaker briefed audience about AI based decision support system, simulation and wargaming software UDAAN (Unit for Digitisation Automation Artificial Intelligence and App Networking) used by Indian Air Force.



- Salient aspects of this system in the field of Command control reporting and air operations monitoring were highlighted.
- Development of ecosystem, in conjunction with MSME/IIT/Universities, outsourcing to vendors/PSU, in house development were also explained in detail.
- Al enabled workstations of different domains such as human, operations and open-source feeds Al enabled fusion and analysis server for further painting a cohesive intelligence picture in ISR domain to facilitate air operations.
- Maintenance management involving one lakh registered users, 25 lakh assets and 85 lakh work orders performed by UDAAN. System also undertakes material management of Indian Air Force with all inclusive logistics support.
- Further an AI based Centre of Excellence (COE) has been established to cover AI based NLP, IACCS, IPSS, Mission planning and wargaming, prediction of operational stamina and AI enabled Intelligence analysis.
- COE further provide admin, operation and maintenance support, and intelligence surveillance during operations.
- Software further assists in forecasting enemy endurance, campaign/mission planning and wargaming.

# Sh Nishant Kumar: Indian Cyber Crime Coordination Centre

- Cybercrimes are omnipresent in our life. The rate at which technology has evolved and the digitalization under which the country has undergone, has opened avenues for innovation and opportunities but at the same time it has also opened door for many types of cybercrimes that are happening today which is also a national threat. After analysis and tracking the incidents of money related frauds, it is observed it is being converted into crypto currency and being utilised by terror funding organizations.
- Al in the hand of attackers also point out what particular vulnerability is in the network and accordingly it can design its attack. Apropos it becomes difficult for a defender to design their tools to counter the threat. Similarly, the malwares have now gone intelligent.
- The most prominent attacks are through- phishing, social engineering, cyber bullying, extortion, sextortion, digital arrest and cyber kidnapping. Recent cyberattacks have been carried out through targeted social engineering. Also, Al enabled attacks are the data manipulation and deep fakes. Al tools which have been developed for the correct purpose, they are also going in the hands of attackers and they are being misused for attacking such type of cybercrime or attack.



- Even in India, we are not having even a cyber police station in all the districts. So, it is very difficult for local police to identify and counter all these types of threats. The defensive mechanism also should be adaptive and innovative.
- In crypto exchange, the future is very challenging with respect to cybercrime because crypto currencies are nowadays becoming a very convenient tool for the cyber criminals. If one goes to the dark web and analyse, it can be observed that most of the transactions are taking place through untraceable entities on such platforms.
- Other technologies which are suspected to be used in cybercrimes are drone technology, cloud technology, IOTs which are going to come very frequently and then generative AI. These will change the domain of cybercrime in near future.

### **Recommendations**

- Research and Innovation- India has to stay ahead of evolving cyber threatsconceptualize what can happen in the next three to five years, then work and promote ethical AI practices to build a secure and unbiased digital ecosystem.
- Reforms and strengthen Law enforcement agencies across the country which will help the police personnel in the investigation process.
- Government department as well along with partnering with the academia and industries to develop counter fail safe mechanisms against evolving cyber threats.

# ROUNDTABLE MEETING 3: LEVERAGING AI FOR MILITARY INFORMATION, DECISION & COLLABORATIVE COMBAT SECURITY

# Key Takeaways from the talk by Commodore T Ajit, Weapons & Electronic Systems Engineering Establishment, Indian Navy

Al systems are growing at a fast pace and introduction of Al will impact the role of specialization for which the officers and men are trained upon. The Al systems have the computational power and the Al tools will not have the same level of appreciation of the weapon systems as a human being. The Dilemma is how much to trust the system and how will the specialization vs Al will address the expertise built in an organization over a period of time.

### Key Takeaways from the talk by Lt Col Abhishek Vardhan

The collaborative systems using AI will be used for new as well as legacy systems. The legacy systems may not be able to integrate AI into their system. How do we handle this issue by optimally balancing these two systems.



# Key Takeaways from the talk by Lt Cdr Abhishek Vardhan, Technology Development Application Cell

Artificial General Intelligence will map the data to derive a solution to a problem. Al General Intelligence maps the data in a 3D vector space and makes a pattern. This system will need learning using the data base. The vagaries of actual combat are vastly different from simulations. Hence, how do we address this issue? The data and intelligence are not connected. Hence, experience will give the dimensionality of the data that can shape our intelligence. There is a need to interface the three services equipment so as to fight together. Application of AI for the military can be in three main areas:-

- Intelligence generation Where the inputs by imagery will give rise to Anomaly detection.
- Use of AI to analyze data and velocity of data on external and internal intelligence being drawn in the system.
- Robotization of soldiers. The Chinese army is making robots to fight. We too must develop robots to fight on our borders.

We must develop AI indigenously. Since we do not have the access to the black box of the systems supplied by foreign vendors, we may not be sure how it will perform under our own combat conditions,

One speaker confirmed that the computing capabilities are available with the organizations and we must develop the decision support systems to fight tomorrow's war.

# ROUNDTABLE MEETING 4: LEVERAGING ROBOTICS AND AI FOR MILITARY SUSTENANCE & LOGISTICS

The 4<sup>th</sup> round of the Round Table Discussion of the seminar focussed on **Leveraging Robotics and AI for Military Sustenance & Logistics**. The RTD was chaired by Lt Gen MU Nair (Retd), National Cyber Security Coordinator. Eminent participants from Think Tanks, Services, (ADB, UDAAN, CME, CAPS) Industry, DRDO and Academia participated in the RTD. Important Takeaways from the RTD are covered in succeeding paragraphs.

The challenges in Army logistics chain due to geographical spread and terrain, constrains were highlighted. Emphasis on the use of AI to optimise the logistics requirements and find solutions to the logistics challenges were highlighted.

<u>Use of Al for Demand Forecast and Warehouse Optimisation</u>. Indian Army is looking at Al based delivery systems. Mobilisation by air, road and Rails resorted to which has its own challenges and results in time delays as it utilises the civil infrastructure and thus Al



solutions to optimise the same needs to be thought of. Logistic Data is generated in very large volumes. Its analysis and utilisation have to be based on digitisation which demands procedural changes. There is a need for collaboration between Army and Industry for finding better solutions to logistic problems for which Govt of India has to lay down the policy guidelines. Up gradation of systems has to be resorted to by the army to use AI tools for logistic solutions. It was highlighted that we are heavily dependent on foreign platforms for AI usage. Automation can be bought from foreign companies but AI tools have to be indigenous.

Automation of **Integrated Materials Management Online system (IMMOLS)** by IAF was highlighted but as far as AI in IMMOLS is concerned, we are far behind. 3 D stereography and image printing of components has been implemented in Air force. Automation and digitisation of storage warehouse is under progress. Near real time asset management of logistics has been achieved however last mile delivery is still an issue of concern for which industry participation is solicited. Challenges of Power supply in field conditions were reflected by the Armed Forces. It was highlighted the civil industry must find solutions for the same if AI has to be optimised for logistics requirements.

### Issues Highlighted by the Industry

It was highlighted that algorithms works multiple time faster if the data is available in the desired manner, however the same is not provided to industry participants in the same manner. There are cost effective solutions available in civil market and the same can be obtained by the Armed forces. There is a hesitation by the Armed forces in sharing of data in the manner the civil industry requires it. However, a point in the case was highlighted where in TCS was hired by Air force to overcome security concerns and digitisation was achieved without compromising the security. The Armed forces must use these types of services from the civil industry.

It was highlighted by civil industry that large number of cost-effective automation tools are available for inventory management and real time inventory monitoring which the Armed forces must utilise. Automation of warehouses by use of low-cost AI solutions is also available which can be made available to the Armed Forces.

Last mile delivery solutions by automated drones and rope ways can be provided by the civil industry in challenging terrain. Large numbers of computer tools are available which can mask the confidentiality of the data and the same can be shared by the Armed forces with civil industry to find solutions to their logistics problems.

# **Recommendations**



It was emphasised that the best practices of automation in logistic systems by three services and civil industries must be shared to overcome logistic challenges. Framework interaction and constant consultation between Armed forces and civil industry must be instituted for finding better solutions to logistic problems. User involvement with civil industry must be encouraged for which HR management by the Armed forces must be implemented for continuity.

# SESSION 5: ETHICAL CONSIDERATIONS AND SOCIETAL IMPACT OF AI IN EDUCATION: ENSURING EQUITY AND FAIRNESS

During Session 5, Brigadier Rohit Chaudhary, SM, Commandant, Wargaming Development Centre (WARDEC) spoke on 'Leveraging Al, Augmented and Virtual Reality in Military Training and Human Resource Development'. Major aspects covered are given in succeeding paragraphs.

For the men in uniform, training forms the backbone of a strong military force, for being ever prepared to carry out its defined operational roles. The changing and uncertain geopolitical construct needs to sustain a technologically driven, meticulously trained and a networked fighting and responsive defence force. This necessitates continuously evaluating and transforming military training methodology along with requisite training and up skilling in niche technology for enhancing technical threshold within the military. For modern day Armies, AI is playing crucial role in military training by simulating realistic scenarios, enhancing decision making skills and providing personalised learning experiences. It enables cost effective immersive training environment that closely mimics real world situations, thereby bringing in greater realism and objectivity. Modern simulation techniques also facilitate in developing near real training applications, which also help in psychological tuning up of soldiers towards elements of combat stress like fear, anger, and shock and so on.

There are numerous advantages as accrued by technology infusion and some of the significant ones are:-

- Al's ability to generate realistic operational training environment facilitates training in a fail safe environment giving soldiers and commanders, experience and confidence required to perform effectively while facing real field scenario.
- A soldier needs to be continuously skilled, at times de-skilled and re-skilled. Technology not only improves overall training efficiency, but also reduces time required for skill development, thereby reducing training cycle, which a soldier has to periodically undergo.
- AI-AR-VR enabled synthetic environment for training, not only obviates employment of original weapons and equipment and movement of troops, but also saves precious time and accruing incidental savings to exchequer.



- Availability of real estate will always be at premium and employment of this niche-field furthermore assists to overcome constraints of availability of ranges or appropriate training areas.
- Technology driven training, facilitates in attaining quantification of not only individuals, but also the collective body of troops by means of objective analysis of After Action Reports.
- Major technological advanced countries including the US, the UK, France, Australia and Singapore have developed cutting edge ecosystem, wherein, 'AI-AR-VR' based training is being leveraged with major impetus being given in the field of Autonomous Systems and Human - Machine collaboration. They have identified key areas for advancement of technology driven training, which includes delivering AI enabled capabilities and cultivating a leading AI workforce, engaging with commercial, academic and partners, maintaining ethical issues while engaging with AI.
- 2024 has been earmarked by the Chief of Army Staff as the 'Year of Technology Absorption'. Five Focus Areas to achieve the set goals are - 'Aligning and Incorporating Technology in Strategic, Operational and Tactical Level', 'Mapping Future and Emergent Technologies', 'Strengthening the Defence Technologies Ecosystem', 'Enhancing Technical Threshold of Our Soldiers' and 'Enabling Techno-Warriors and Commanders'.
- To enhance technology threshold and training within the forces, AI has now been placed at the 'Centre of Quest for Military Modernisation and Capability Development'. A number of Centre of Excellence Institutes have been nominated with aim of researching technology, identifying applications and finding solutions to enhance military capability. Key areas of application have been identified covering the entire canvas of operational, training and logistics domain. These include Intelligence Surveillance Reconnaissance (ISR), AI enabled Drones, Intelligence Fusion, Threat Assessment, Cyber Security, Data Analytics, Computer Wargaming, Logistics and Healthcare.
- Computer Wargames along with simulator-based training has been at forefront for leveraging technology in military training. The concept of integration of three realms of simulation of Live-Virtual-Constructive-Integrated-Architecture has brought in greater realism and accuracy in training, as also achieve the goals of increased efficiency, improved outcome and become less manpower intensive.
- To adapt the transformative and rapid advancing technologies, Indian Army is readapting its culture, skill and approaches by synchronising the triad of people, processes and technology. For it, skilled HR is necessary to ensure continuity in thoughts and actions. The basic tenet of HR skilling follows a three-pronged approach with levels graduating from attaining basic awareness, enhanced learning and advance learning, there by touching upon the complete spectrum of hierarchical structure creating a skilled pool of human resource with varying level of expertise.
- The basic awareness for all especially officer cadre aims at imparting basic knowledge through conduct of self-learning through online customised courses as also short re-



orientation capsules at various courses of instructions a uniformed person attends during his career in the Army. The end state is to develop a basic knowledge platform which acts as a harbinger for future enriched learning process.

- For enhanced learning, customised subjects as electives in engineering degree courses are being leveraged for solving existing problems and optimising solutions. Customised emerging technological courses with appropriate learning value is facilitating in creation of in-house intermediate experts.
- For advanced learning, expertise in identified specialist verticals such as UAVs/ RPAs/Drones, ISR, Cyber, EW and IW is being acquired by pool of subject matter experts with domain specialisation, by pursuing higher studies to include postgraduation, PhD on projects aligned to military use.
- Training and skilling in this niche technology is an important prerequisite for imbibing, enhancing the technological threshold within the Army and exploiting it in an appropriate manner to accrue maximum benefits. Leveraging AI-AR-VR in military training is essential to lead the Army on its 'Path of Transformation'.

# SESSION 6: AI IN PUBLIC HEALTH AND DISEASE SURVEILLANCE: ENHANCING PREVENTION AND PANDEMIC PREPAREDNESS

# **Robotic Surgery and AI: Present and Future in Military Health Services**

During Session 6, Colonel Amit Shah, Head of Department of Urology, Army Hospital (Research and Referral) spoke on '**Robotic Surgery and Al: Present and Future in Military Health Services'**. The important aspects covered by him are given in succeeding paragraphs. A humble beginning around 10 years back read 'Taking Surgery Beyond Limits of Human Hands' and now Robotic Surgery can be termed as a perfect combination of Human Skill and Mechanical Precision. Therefore, it is always a Robot Assisted Surgery, wherein, the surgeon performs the surgery and the robot only assists him.

With rapid advancement and extending life expectancy, we are at a crucial cross road of medical care, where we cannot stay with conventional medical practice and have to adapt with evolving technology to win the race against the diseases. So, surgeons have tough task awaiting them, but a surgeon never gives up and always tends to master his skills.

All the wars have brought in something new to the surgical field. A brief study of history will make us understand that the concept of Robotic Surgery has arisen from Battlefields and Space Stations. In earlier days, when Robotics were being introduced, then the glamorous field of Surgery Neurosurgery and Cardiac Surgery got the chance to experiment with it, however it was Urology Branch, which grabbed the opportunity probably because field of urology appeared to be favourable for Robots: a deep pelvis, deep prostate, mobile urinary bladder or kidneys held only on vascular pedicle.



The present Robotics work on the Master Slave Concept and it's a real wonder as it offers seven degrees of freedom, which emulates a wrist inside the body cavity with a 3D magnified vision. With this the advantages of Robotic surgery are self-explanatory. The journey and advancement in field of Robotic Surgery in India has been exponential and it has been mostly with the corporate set up and government set up has somehow lagged behind. Because of certain inherent issues on procurement especially delisting Robotic Surgery platform from Make in India Exemption List has only added to already troubled waters. Future is waiting with advancement, incorporating AI, reduction in cost and multiple players dominating the field of surgery, but there is a need to adopt and advance further.