MANEKSHAW PAPER No. 75, 2018

# Autonomy and Artificial Intelligence:
## The Future Ingredient of Area Denial Strategy in Land Warfare

Debasis Dash

Centre for Land Warfare Studies
New Delhi

KNOWLEDGE WORLD
KW Publishers Pvt Ltd
New Delhi

ISSN 23939729

**Centre for Land Warfare Studies**
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone: +91.11.25691308 Fax: +91.11.25692347
email: landwarfare@gmail.com website: www.claws.in
CLAWS Army No. 33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent think-tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.



Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore, may not be quoted or cited as representing the views or policy of the Government of India, or Integrated of the Ministry of Defence (MoD) (Army), or the Centre for Land Warfare Studies.

KNOWLEDGE WORLD

www.kwpub.com

Published in India by

Kalpana Shukla
KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110002
Phone: +91 11 23263498 / 43528107 email: kw@kwpub.com • www.kwpub.com

# Contents

# List of Abbreviations

| Acronyms | Full Forms |
|---|---|
| A2 | Anti-Access |
| ACCCS | Artillery Combat Command and Communication System |
| AD | Area Denial |
| ADCRS | Air Defence Control and Reporting System |
| AFRL | Air Force Research Laboratory |
| AGI | Artificial General Intelligence |
| AI | Artificial Intelligence |
| ANI | Artificial Narrow Intelligence |
| ASI | Artificial Super Intelligence |
| ATGMs | Anti-Tank Guided Missile System |
| ATR | Automatic Target Recognition |
| BMD | Ballistic Missile Defence |
| BMS | Battlefield Management System |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance |
| CAPF | Central Armed Police Forces |
| CBI | Central Bureau of Investigation |
| CIDSS | Command Information Decision Support System |
| CIWS | Close in Weapon System |
| CSBA | Centre for Strategic and Budgetary Assessment |
| DACO | Defend and Control |
| DARPA | Defense Advanced Research Agency |
| DCN | Defence Communication Network |
| DEFT | Deep Exploration and Filtering of Text |
| DoDP | Department of Defence Production |
| DoEx | Department of Ex-Servicemen |
| DRDO | Defense Research and Development Organisation |
| DRI | Directorate of Revenue Intelligence |
| DNSA | Deputy National Security Advisor |
| ELINT | Electronic Intelligence |
| EWS | Electronic Warfare Systems |
| GPS | Global Positioning System |
| GWOT | Global War on Terrorism |
| HAL | Hindustan Aeronautics Limited |

| | |
|---|---|
| HQ | Headquarters |
| HUMINT | Human Intelligence |
| I2O | Information Innovation Office |
| IAI | Israeli Aerospace Industries |
| IB | Intelligence Bureau |
| IDS | Integrated Defence Staff |
| IRNSS | Indian Regional Navigation Satellite System |
| ISR | Intelligence, Surveillance and Reconnaissance |
| IW | Information Warfare |
| JCB | Joint Cypher Bureau |
| MAC | Multi Agency Centre |
| MANPADS | Man Portable Air Defence Systems |
| MEA | Ministry of External Affairs |
| ML | Machine Learning |
| MoD | Ministry of Defence |
| MHA | Ministry of Home Affairs |
| MRO | Maintenance, Repair and Overhaul |
| NATGRID | National Intelligence Grid |
| NCB | Narcotics Bureau |
| NCW | Network-Centric Warfare |
| NIA | National Investigation Agency |
| NLP | Natural Language Processing |
| NSA | National Security Advisor |
| PMO | Prime Minister's Office |
| R&AW | Research and Analysis Wing |
| RCV | Remotely Controlled Vehicles |
| RDECOM | Research, Development and Engineering Command |
| RMA | Revolution in Military Affairs |
| ROV | Remotely Operated Vehicles |
| RSA | Revolution in Strategic Affairs |
| SACLOS | Semi-Automatic Command Line Of Sight |
| Tac C3I | Tactical Command Control Communication and Information System |
| UAS | Unmanned Autonomous System |
| UAV | Unmanned Aerial Vehicle |
| UGV | Unmanned Ground Vehicle |
| VSHROAD | Very Short-Range Air Defence |

# Autonomy and Artificial Intelligence:
## The Future Ingredient of Area Denial Strategy in Land Warfare

### Introduction

Any innovation, whether its technological or doctrinal, that is meant to infuse a considerable change in the method of warfighting while improving the overall capability of a military force is part of the concept of 'Revolution in Military Affairs (RMA)'.[1] For that reason, the advancement in computational power, evolution of microelectronics and miniaturisation of computing chips have brought in a transformative change in the way a warfighting strategy is developed and sustained. This has also led to the development of the concept of Network-Centric Warfare (NCW). Hence, the current debate around the use of autonomous weapon platforms and artificial intelligence (AI) applications to dominate the future battlefield has been central to the realisation of that concept of NCW. Unlike its traditional counterpart, that is, platform-centric warfare, in which the effectiveness of any particular type of weapon platform dominates the outcome, NCW was meant to form a network of connected devices, each acting as a source of information, and also as an agent of action in a combat environment. The intention was to create an intelligence grid, both flexible in its scope and scale, and to have force superiority as well as information dominance in the battlefield.

The underlying philosophy at the core of the concept is that of Observe, Orient, Decide and Act (OODA) cycle, that describes the stages involved in initiating any military manoeuvre at all levels of warfare (tactical, operational and strategic).[2] The OODA loop is meant to achieve higher operational tempo in an event of war by synergising engagement among multiple nodes of operations into a collective effort and direct them toward a common goal. While the first three stages, that is, Observe-Orientate-Decide involve collection, collation, processing and analyses of the information received from various sources that include battlefield surveillance radars, unmanned sensors, Unmanned Aerial Vehicles (UAVs), Unmanned Ground Vehicles (UGVs) and human sources to provide a comprehensive view to the commanders at different levels for effective decision-making, the last stage is to implement the decision that is to 'act' using different warfighting components (artillery guns, missiles, air defence systems, etc.) at their disposal. Both the concept

of autonomy and AI are meant to augment the four stages of OODA cycle.

In this paper, I have discussed the concept of autonomy that explores the utility of various platforms in augmenting the army's Area Denial (AD) strategy while providing a comprehensive picture of the use of automated platforms such as UAVs, UGVs and sensors across different missions such as Intelligence Surveillance and Reconnaissance (ISR) operations, battlefield management, border patrol and so forth. The factors responsible for their deployment are discussed as well. The applicability of the concept of AI has also been discussed in detail and the security architecture has been provided with a particular focus on its use in the Indian army. Various subareas of AI having relevance to defence and security applications are explained with real-life examples. The chapter on the strategy of AD provides an overview of its usage in the context of land warfare. In it, the evolution of the concept of Anti-Access Area Denial (A2/AD) and its contemporary parlance in Indian army has been discussed. Also, the chapter contains the details of types of adversaries linked to the A2/AD concept and the categories of weapon profiles that have been developed over time to put the concept into practice. The last chapter of 'Autonomy, AI and Army (3A)', analyses the application of the two concepts with respect to Indian army and the possibility of building the capability on the current communication and control structure.

## AI in Defence: Concept and Utility

> Now the reason the enlightened prince and the wise general conquer the enemy, whenever they move, and their achievements surpass those of ordinary men, is foreknowledge
>
> —Sun Tzu, The Art of War[3]

In modern warfare, expansion of the battlefield transcends beyond the conventional domains of air, sea, land and space, into a dimension crowded with information. This extension facilitates manipulation of the enemy's cognitive behaviour, penetrates into its security systems and triggers system-wide attacks, thereby posing a threat to its critical infrastructure. All this has been categorised as information warfare (IW) that has further accelerated the RMA. However, this in no way has made other forms of traditional warfare lose their relevance but has graduated to the next level, where the fifth dimension, that is, cyberspace will be at the core influencing the outcomes of a war.[4]

In the case of war, apart from men and equipment (weapons and platforms), management (higher defence management) plays an important role across all levels (tactical, operational and strategic) of battle. The management is backed by intelligence apparatus and oversees the entire command and control of

the formations right from the strategic to tactical level. This has brought the onus of efficient and optimum decision-making on commanders across all the levels, from a unit to that of an operational command. Interestingly, this imperative has led to a change in thinking at the strategic level, effecting a Revolution in Strategic Affairs (RSA).[5] But for efficient decision-making, there has to be a support system that provides the basis for further analysis. In military parlance, this is classified as 'intelligence' received from a web of electronic sensors (known as electronic intelligence [ELINT]), a network of informants and through human intervention (also known as human intelligence [HUMINT]). This very act of the collection, collation and classification of the intelligence received, can be done via algorithms through supervised (human guided) and unsupervised (self-trained) learning methods in order to provide decision makers (commanders) with the patterns of occurrence of events giving them a larger picture of the evolving situation for efficient decision-making. This is the kind of the foreknowledge that can prevent any major unwanted failures. Hence, in our context, the foreknowledge, that is, 'intelligence (information)' and the algorithms that skim them, to process and provide a meaningful observation, are called AI.

***AI and Their Levels***

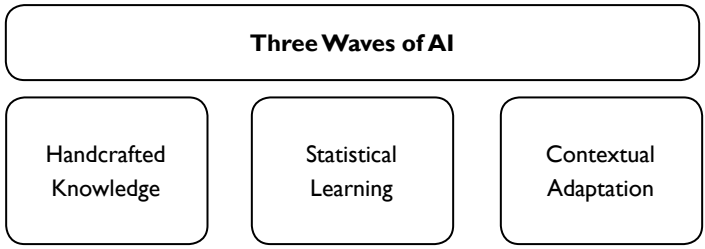
The study on AI started around the Second World War, with the design of 'Boolean Circuit Model of Brain' by McCulloch and Pitts.[6] This was followed by the publication of a paper titled 'Computing Machinery and Intelligence' by Alan M. Turing, proposing the plausibility of intelligence in machines based on the 'imitation game'. In the game, a digital computer outsmarts a human interrogator in solving simple riddles, setting the course for further research work on AI to explore the extent to which machines can replicate and not just imitate the HUMINT.[7] However, it was in 1983 that the US Army Sciences Board, in one of its study, hypothesised that machines can have the capability to extract and interpret information for decision-making that resembles the sophistication of the HUMINT. In their latest report, the board has further echoed its ambition to the scale of achieving the level of AI close to the human thinking ability.[8]

But the realisation of the concept into defence applications has to pass through different stages of development. According to John Launchbury, Director of Information Innovation Office (I2O) from Defence Advanced Research Agency (DARPA), the consummation of AI into something usable will occur in three waves.[9]

These three waves of development are intended to train the algorithms and computing systems to perform simple tasks such as calculation of

numbers, matching colours, playing games and so forth, and gradually take up assignments that transcend basic HUMINT. In the first wave, rules based on logic were codified by the domain experts and were then fed into computers to follow the rules and process the data that was made available from cloud-enabled networks. It was evident from systems such as 'AlphaGo' software developed by Google that defeated a 19-year-old professional Go player from China[10]. This was its second victory, with first being against Lee Se-dol from South Korea.[11]

**Figure 1. The DARPA perspective of Artificial Intelligence (AI).[10]**



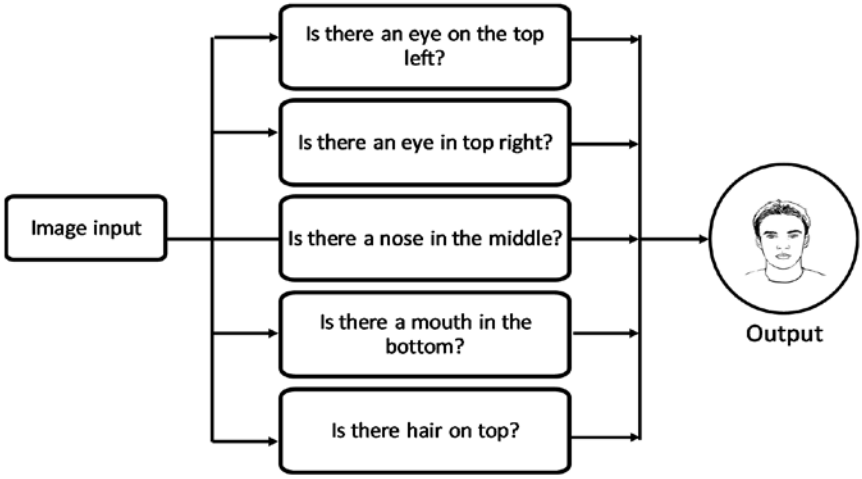

The first wave AI systems were of great help to study computer networks, identify the vulnerabilities and devise ways to fix them (e.g., securing mission-critical networks). At this level, the AI systems had a fair amount of perception and reasoning capabilities but lacked entirely in abstraction and learning. These systems were decent enough to solve narrowly defined problems with the fair level of reasoning but were incapable of handling the uncertainty.

In an attempt to further improve the learning ability of the algorithms, the second wave took the course of statistical learning. The statistical learning involves developing an algorithm and training it with different data sets by weeding out errors in each iteration to make the programme work in an efficient manner. Some of the common tasks that use statistical learning methods are handwriting recognition, facial recognition, voice recognition and vision-guided navigation used in autonomous ground vehicles. The algorithms are trained using the concept of neural networks, (to be discussed later in this chapter). This involves identifying the problem (say, face recognition) and then break it down to mathematical equations that makes the basis for developing logics on which the ML algorithms are written and trained with varied data sets.[11, 12] While the learning method improved the perceiving (observing and taking inputs from the surroundings through sensors) and learning ability of the AI system, it failed to enhance the abstraction (applying the learning in different contexts) and the reasoning ability.[10]

The third wave of AI intends to remove the technological challenges encountered in the second wave to truly help machines imitate HUMINT,

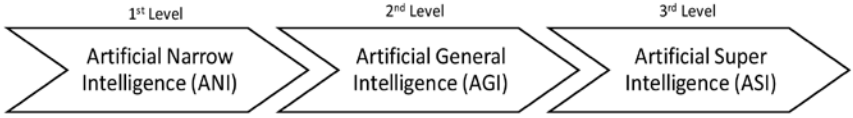
by helping them with 'contextual adaptation'. Contextual adaptation helps machines to make use of their learning (understandings from training with varied data sets) to draw an analysis from any given problem or a situation and decide or suggest an appropriate course of action or a probable solution. In short, they make machines more reflexive than reflective. There are certain AI-based applications as analogous to 'Chat Bots, such as Tay Bot[13] and Virtual Personal Assistants' such as Siri, Cortana, Google Assistant and so forth. But their limitation is that they answer a query by matching it with their available database while failing to generate an innovative answer on their own to any random query or event thrown at them. The perfect case was of Tay AI twitter bot by Microsoft Corporation, which was closed down because of its failure to identify the context while responding to queries on its Twitter page, as a result, it ended up repeating others' comments as answers to the queries thrown at it[14]. Therefore, the third wave aims at implementing contextual adaptation through algorithms that are designed to construct 'self-explanatory models to understand real-world phenomena'.[9] Below is an explanatory model designed to train an algorithm for a face recognition task

**Figure 2. Face recognition using deep learning.[12]**




However, acquisition of the true form of HUMINT will be happening in three levels namely, Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI) and Artificial Super Intelligence (ASI). In this, each level will develop a certain degree of technological capability while advancing towards the ultimate goal. These three levels are also critical to the development of various systems and platforms for defence and security applications as much as they are for non-military and commercial applications.

**Figure 3. Three levels of AI.**[15]




The first level is called 'ANI'. At this level, computing systems are given access to information repositories and are trained to perform specific tasks involving data collection and analysis on their own, taking over the tedious calculations and relieving their human counterparts to do complex tasks that involve a high degree of abstraction. In defence and security applications, ANI is used across weapon platforms such as anti-missile cannons (e.g. Phalanx Close-in Weapon Systems [CIWS]), target acquisition and flight course correction for anti-tank missiles, missile guidance in Ballistic Missile Defence Systems (such as Patriot BMD)[16]. Other examples of non-military and commercial applications include online translation software (Google translate, Bing translate) and computing systems (Deep Blue, Watson and AlphaGo)[17]. Every intelligent system has some degree of autonomy inbuilt with which it executes the task. Moreover, a weapon platform operating either in semi-autonomous or autonomous mode can be part of ANI. One such example can be of newly developed Amogha-II Anti-Tank Guided Missile System (ATGMS) by Bharat Dynamics Limited. Its Semi-Automatic Command Line of Sight (SACLOS) system ensures that the missile keeps itself on the target's line of sight while automatically adjusting its flight course[18]. Interestingly, Amogha-II is a semi-autonomous version of Amogha ATGMS weapon platform, which further confirms the fact that intelligence can be brought into older platforms.[18]

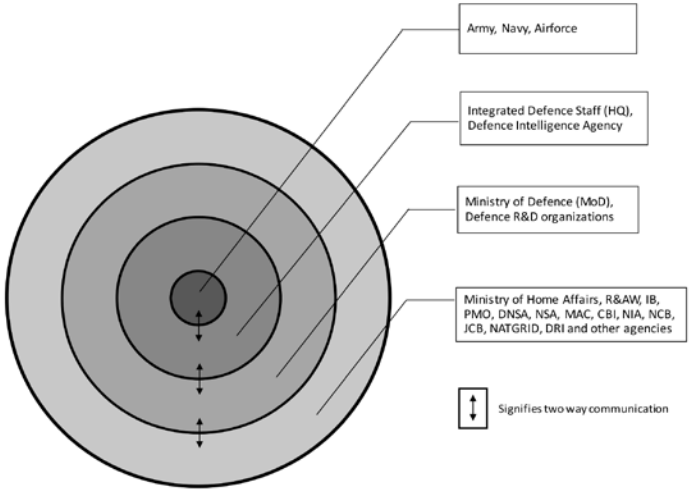
The second level of the revolution for achieving HUMINT in machines is called AGI. AGI intends to enhance the learning ability of algorithms to accomplish a large number of tasks that are basic in nature, but part of the overall HUMINT.[15] This can be best explained through an example. Imagine a hostile environment where a robotic system running algorithms, identifies a rifle on its own, picks it up, scans the surrounding, identifies the enemy and opens up the fire. Here, the job of identifying a rifle, its parts, cocking it up and figuring out the trigger involves intelligence. Now, this act is not done through a simple process of data collection, analysis and action, rather the algorithm does a deep inward search into its networks, pulling information from a web of other networks and subnetworks to be able to understand and identify the rifle and its parts[19]. While considerable success has been achieved in realising ANI, the development of AGI is still a work in progress. The biggest challenge is to enhance the capability of the neural networks to connect with various other neural networks across different systems

to work in collaboration while executing an act of general intelligence. In short, this means 'cross-domain use of acquired intelligence'.[19] A most recent example can be of 'PathNet', a general intelligence architecture published by Google's DeepMind, which combines different ML techniques to train its neural networks.[20–21] Interestingly, use of AGI systems and algorithms are field neutral and can be used across both military and non-military applications, making it easy to absorb the technology concept into defence and security-related applications, once it is validated.

The third and final destination of AI revolution is named as ASI. It is the point at which machine intelligence exceeds HUMINT both qualitatively and quantitatively[22]. Even though at present, ASI is a concept, but the fact is that human memory has its own biological limitations in terms of forgetfulness, distraction and degeneration, whereas a memory built upon semiconductor units is both scalable and flexible. The underlying concepts of neural networks, learning techniques and database remain key to the growth of ASI and the former is largely dependent upon the sophistication of those underlying concepts. However, given the level of dubiety with regards to a combination of ASI with defence and security applications, we are yet to see what kind of tasks are entrusted to ASI in the days to come.

### *AI in National Security Architecture*

**Figure 4. Four-tier communication channel in defence and security architecture for implementation of AI.[23]**

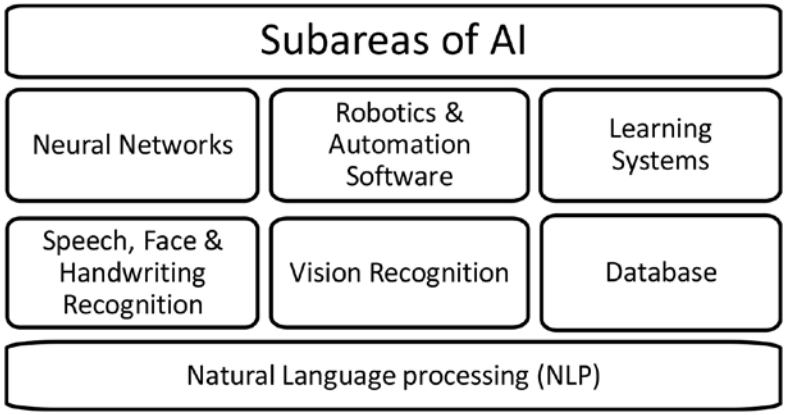



The role of AI in defence and security architecture is multitudinous. It can be used for gathering, collating and disseminating information across

different tiers, depending upon the type of information required and using certain types of equipment deployed in the field through a remote command post. In the above picture, key elements of India's defence and security architecture have been classified into four tiers, with each having their own area of operation and expertise. The objective is to use AI as a tool to integrate organisations that were working in silos into a single structure for effective command and control. The first tier consists of armed forces, that is, army, navy and air force. In this tier, each of the tri-services operating their own database over the cloud infrastructure is made to share mission-critical information both within and across the services on a need to know basis. In the second tier, there is Integrated Defence Staff (IDS) whose main objective is to bring cohesion to the three services. Here, the information meant for joint operations is received and processed. This is a two-way channel, with each tier communicating with the other. The third tier consists of Ministry of Defence (MoD) and its satellite departments (Department of Defence [DoD], Department of Defence Production [DoDP] and Department of Ex-Servicemen [DoEx]). At this tier, data related to weapon procurement and acquisition, defence management, strategy and so forth, is collected, collated and shared as per the need. But apart from that, this tier provides an excellent opportunity for policy research and planning. In the fourth tier, critical information fromMHA, Ministry of External Affairs (MEA), Intelligence Bureau (IB), Research and Analysis Wing (R&AW), Central Armed Police Forces and other financial intelligence and security agencies is collected and processed. It is an important part of the overall security architecture. At present, National Intelligence Grid (NATGRID) is tasked with the responsibility to collect, collate and analyse data from various law enforcement agencies, financial institutions as well as the private sector, and can be linked to the fourth tier[24]. Another interesting observation will be mapping the three levels of AI against the four tiers of the security architecture. The first tier will use ANI for gathering and analysis of the data from its sensors and men on the ground while keeping AGI restricted to the analysis of the historical data, identification of patterns and training its algorithms. The data received from the first and the second tier will be used by the third tier at ANI and AGI level, for long-term policy planning and identify opportunities and challenges. The fourth tier will follow the suite as that of the third tier but may think of using ASI level for policy planning and recommendation purpose.

*Subareas of AI Relevant to Defence and Security Applications*

**Figure 5. Subareas of AI relevant to Defence and Security Applications.[25, 26]**



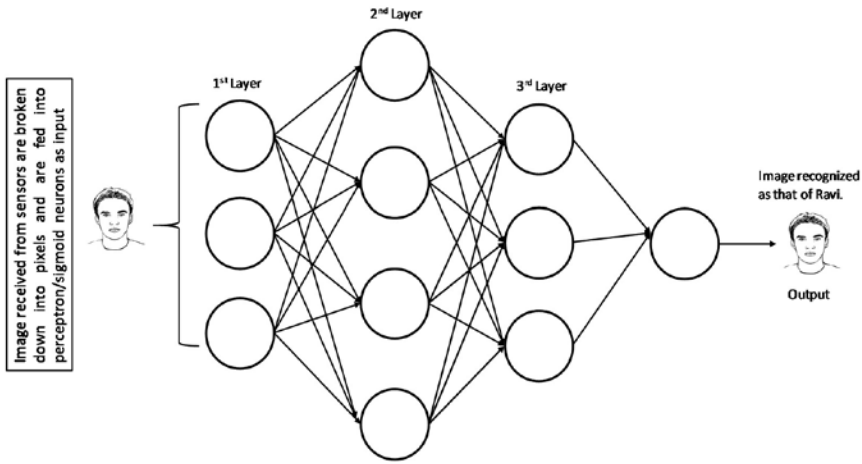

AI, as conceptualised to imitate and function ahead of HUMINT, is not a single entity or made up of any single technology, rather similar to its biological counterpart, it is made up of many different technologies that when working in coordination, give rise to an intelligent behaviour. The intelligent behaviour may include accessing information from a database, processing, matching, recognition of patterns and so forth. In addition to the above tasks, they have to train and retrain themselves much like a human brain, which replaces old data with new information.[21] The AI system consists of different subareas, however, only those with relevance to defence and security applications are discussed here.

## Neural Networks

The concept of neural networks is drawn from the arrangement of neurons inside a human brain that receives, processes and transmits information to a network of nerve cells executing the task of learning and reasoning. A neural network consists of many small units, categorised into two types namely, perceptron and sigmoid neuron. For a deeper understanding, an artificial neuron (perceptron or sigmoid neuron) is a mathematical function conceived on the model of a biological neuron[11]. Their job is to receive information from various input sources (e.g. sensors) and process them and they are only responsible for training neural networks with different data sets for the purpose of learning. A typical neuron network may include many layers of filters, across which an input is passed through selectively based on some parameters. The algorithms that are used to train neural networks are called Stochastic Gradient Descent

and the technique used in their training is called backpropagation. The main objective of backpropagation is to keep track of probable changes happening across the layers. The following example shows the process of image recognition and the internal structure of a neural network. In the picture shown below, an image as captured by sensors was broken into pixels and then fed as input to a neural network. On receiving input, the neural network runs the algorithms, matches each pixel of the image with its database and gives output as an identified image of a person named 'Ravi'. Neural networks are used for various other tasks such as character recognition, pattern identification, matching, selection of artillery targets, flight path correction of an ATGM and so forth.

**Figure 6. Neural network for image recognition.**[12,28]

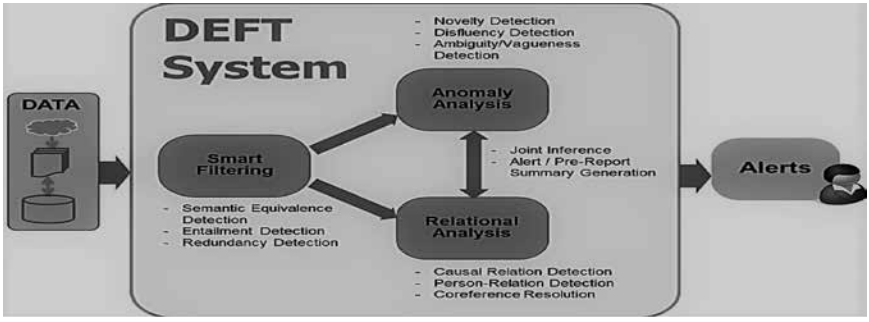



## Natural Language Processing (NLP)

NLP is a subarea of AI which creates an interface between man and machine. It helps the latter understand the human language both in terms of meaning as well as context and initiate 'normal' conversations with the former[27]. The processing of a natural language (e.g. Hindi, English, Odia, French, etc.) is carried out in four stages, that is, signal processing, syntactic analysis, semantic analysis and pragmatic analysis (contextual analysis)[28]. Signal processing involves the conversion of a natural language into the machine-readable language (American Standard Code for Information Interchange (ASCII) characters) and helps a computer categorise the output from the first stage for further analysis. At this stage, the data containing natural language can be obtained from a database on a cloud platform. The second and third stages (syntactic

and semantic analysis) are carried out in tandem as they are interwoven in terms of their end objectives. The syntactic analysis involves breaking of a long sentence into individual components (words and phrases) and testing them against established rules of grammar of the respective natural language, to ensure the sentence is grammatically correct. Pragmatic analysis or contextual analysis is the final stage of NLP that ensures that the words and phrases in a sentence are used appropriately and reflects the context. NLP can be used in studying loads of documents containing critical data and deliver information as per the need of the user. In the case of defence and security, NLP can be used by intelligence and defence analysts for obtaining essential information and relevant patterns from logbooks. One such example is Deep Exploration and Filtering of Text (DEFT), designed by DARPA[29]. DEFT is meant to harness the power of NLP to investigate, analyse and generate data that can be used in the assessment and planning of future operations. Such kind of technologies can be used by intelligence teams operating at a divisional level to support the decision-making process.

**Figure 7. Deep exploration and filtering of text**.[30]




## Speech and Handwriting Recognition

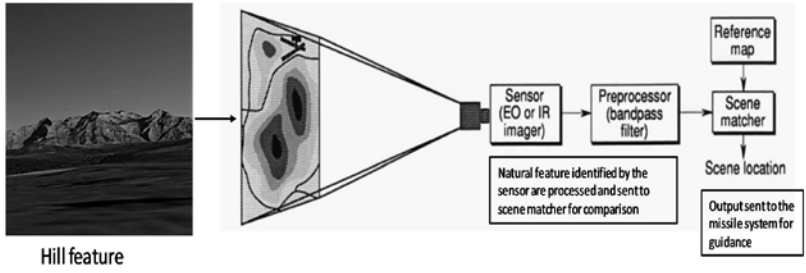
Speech and handwriting recognition are two different subfields under the broad concept of AI, with both sharing the concept of neural networks (as discussed above) as their core learning technology. Speech recognition (SR) involves identification, translation and generation of an output based on the desired language, with an input from a different language. It is also used for the conversion of voice files into text for further analysis. The process of SR to the final output is done in three stages: SR (identification of language/ voice), speech analysis (conversion of natural language into machine-readable language, parsing and matching of speech components) and speech synthesis (generation of speech in the desired language)[31]. On the other hand, handwriting recognition follows the concept of image processing and analysis, in which an

image of a digit is divided into pixels and is fed into neural networks for training purpose. Additionally, various image patterns of the concerned digit are used as a training data set, to make the neural network identify and generate the digit without any error.[12,13] Both speech and handwriting recognition have proved their usability over time. SR was used by the US military on many occasions, including the army doctors to prepare medical instruction manuals in Dari language in Afghanistan and the same was also used during in-flight and ground operations, as suggested by Research, Development, and Engineering Command (RDECOM). Whereas, handwriting recognition forms an important part of NLP and is of great help in identification of texts, digits and symbols from an image and provide NLP with an input.[32,33,11,29]

## Vision Recognition

Vision recognition technology uses a similar concept for training its systems as with speech and handwriting recognition, however, this subarea of AI deals with the recognition of human, animal and natural features. The level of training is quite high, as the data sets used in training the neural networks are based on fractal modelling (modelling of natural features that includes mountains, hills, land surface, coastline, etc.). Fractal modelling involves constructing a fractal model using mathematical equations that describe any naturally occurring fractal. Fractals are hypothetical figures with an irregular geometry and can collectively represent any physical feature or an object. These fractal models are used to provide input to Automatic Target Recognition (ATR) systems that can help in guiding a missile autonomously. The process of ATR involves constructing a fractal model of a battlefield or a theatre, train the neural networks with data sets and initiate the process of scene matching to compare real-time data obtained from sensors with that of stored data for in-flight course correction of the missile[34]. In addition to the missile guidance, vision recognition can be used for navigating the unmanned autonomous vehicle on a battlefield or in an unknown terrain. Below is an example of the vision recognition system for missile guidance.

**Figure 8. Scene matching for missile guidance.**[36]



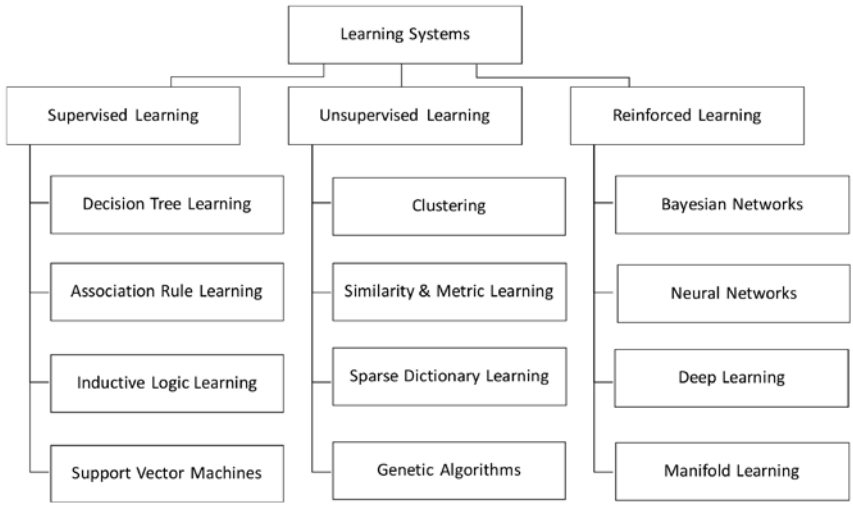
## Automation and Robotics

Automation and robotics are two different subareas of AI, but are closely interlinked, with the latter being a subset of the former in terms of application. The objective of having automation in defence is to enhance operational efficiency, improve situational awareness, ensure low turnaround time for weapon platforms and force readiness[35]. While automation has been part of forth industrial revolution and military operations for quite some time, it is the advent of AI that is about to revolutionise the way automation is implemented[36]. The three such areas in defence application that are likely to have the benefits of AI include cybersecurity, UAS and Maintenance, Repair and Overhaul (MRO) of weapon platforms[37]. In cybersecurity, the power of AI can be used for initiating automated system vulnerability check and respond to an identified cyber-attack based on ML.[9] Also, unmanned autonomous systems such as UAVs and UGVs can be used for Intelligence, Surveillance and Reconnaissance (ISR) and offensive operations through command and control systems backed by AI[38]. One such example is of AI-backed UAV command and control system designed by Psibernetix that outperformed the aircraft control systems used by Air Force Research Laboratory (AFRL) during a simulated offensive air battle[39]. Interestingly, the MRO operations that ensure serviceability and turnaround time of weapon and logistic platforms have a close link with industrial manufacturing. Hence, in this case, collaborative robots can be used alongside maintenance personnel to fasten the process of repair and maintenance[40].

## Learning Systems

Learning systems, also known as ML, are critical to the implementation of AI. They include methods and procedures that are used to develop models using different data sets to imitate HUMINT. ML is broadly classified into three modes of learning—supervised learning, unsupervised learning and reinforced learning. Supervised learning involves developing models based on known input and desired output, with errors generated at each iteration getting incorporated to fine-tune the final output. In unsupervised learning, models are developed to draw inferences and observe patterns from a tranche of data sets as input. On the other hand, in reinforced learning, an analysis model is designed and trained to behave or respond in a particular way based on trial and error process.

**Figure 9. An overview of types of learning systems.**[41]




## Database

The database is an essential requirement and is classified as a subarea of AI. Data comes in varied shapes and sizes and may contain text, videos, audios and images or may be hybrid in nature. It is the collection of different types of data that forms the basis of the knowledge base. However, a raw data is both complex and difficult to interpret, hence it is clustered, cleaned and categorised before any extraction of meaningful information is done.

**Figure 10. Processing of raw data and knowledge creation.**[42]

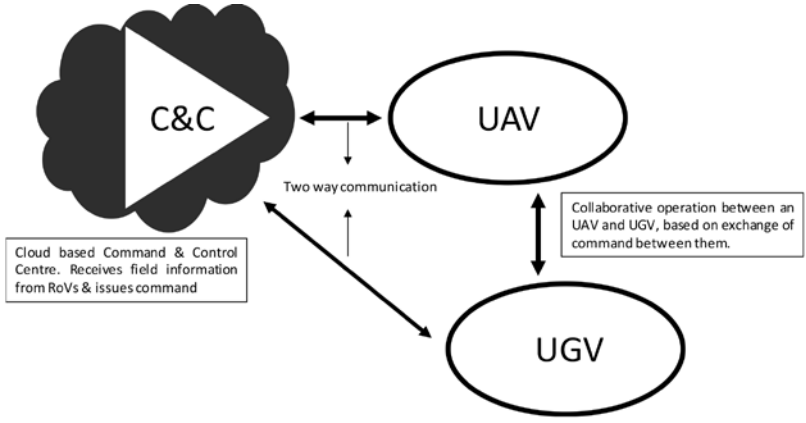

## Autonomy in Defence: Concept and Its Use in Land Warfare

> A Revolution in Military Affairs (RMA) is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations
>
> —Andrew Marshall[43]

The path to a decisive military victory or a stalemate under subtle acceptance of either capability to deter both in defensive and offensive terms largely depends on the way an army manages to employ and deploy its 3Ts in different permutations and combinations. These three Ts are technology, terrain and tactics. This 3T concept has been in use since ages, with militaries over time adopting different technologies to outsmart their adversaries in any given terrain with well-thought-out tactics. An Israeli military historian and theorist, Martin van Creveld in his book 'Technology and War' has mapped this adaptation for warfare across four ages—Age of tools (till 1500 AD), Age of Machines (1540–1830), Age of Systems (1830–1945) and Age of Automation (1945-till date)[44]. Hence, the debate over the concept of autonomy in land warfare is nothing new, rather an elevation in our thought of warfighting to protect our territorial sovereignty.

The concept of using weapon systems with no or under indirect supervision of a soldier has its origin in World War II when teleoperated tanks (teletanks) and Goliath tracked Remotely Operated Vehicles (ROVs) made their debut in the battlefield.[45,46] This led to the advent of ROVs in all dimensions of warfare. However, the relevance of ROVs and the concept of autonomy took precedence as the conceptualisation of NCW gained interest among the military community for varied reasons such as low battlefield casualty, better resource for intelligence gathering and deep strike. The concept of NCW begins with the creation of an intelligence grid from tactical to the strategic level. ROVs and other autonomous systems that include sensor and weapon platforms, form an integral part of this grid through which NCW takes a definitive shape.[47]

**Figure 11. Unmanned systems as part of command and control system.[48]**



### *Types of Autonomy and Platforms*

Autonomy is a concept which when integrated into machines in different ways, exhibits the property in varying degree. Technically, the concept of autonomy is implemented in four modes namely, tethered, remotely controlled, semi-autonomous and fully autonomous.

### Tethered

Tethered systems are connected to a controller or a user device through a wire, eliminating the need for onboard power systems. But this arrangement comes at a cost, with tethered robotic vehicles having restricted to limited movement.[49] Such systems are used for military operations such as explosive and ordnance detection as well as disposal, seabed mapping, water clarity measurement and so forth.[50]

### Remotely Controlled

Remotely controlled vehicles (RCVs) are operated either through radio frequency link, infrared link or wirelessly controlled. Unlike tethered systems, they lack autonomy in terms of operations and decision-making but their movements are not limited.[51] They can move freely across any terrain, given that they stay within the communication range.[52]

### Semi-Autonomous

Semi-autonomous systems have a fair degree of autonomy to execute certain tasks such as obstacle detection and negotiation, border patrol and so forth, with an active or passive involvement of human operators.[53] These systems have an onboard computer system to venture out, collect information and send them back to the control station for processing.[54] This is the most preferred mode of operation by military operators as they continue to control the overall mission execution. However, the human error continues to be a factor. Overall, semi-autonomous robotic systems are preferred because they require less bandwidth for control and command and the amount of data generated is manageable without the need for huge storage. Sustainability of systems under critical missions stands high.

### Fully Autonomous

Systems with an autonomous mode of operation have a high degree of autonomy and the technological capability to sense, gather, collate, process and communicate the information received from the surrounding. They execute tasks based on the type of algorithm coded into their systems. For example, an autonomous Unmanned Combat Aerial Vehicle will only fire missiles if the data taken from surroundings satisfies its decision-making

system (algorithmic flowchart) of the target to be a friend or a foe. This kind of self-decision-making is called 'situational understanding'.[50] Situational understanding of an autonomous robotic system depends upon the quality of its sensors, algorithm to implement AI and a database.

While the concept of autonomy in unmanned systems with different modes of operation is discussed above, the platforms on which they are built are of two types namely, custom-built unmanned systems and Applique Systems. Custom-built unmanned systems are designed and developed to perform a specific set of tasks such as reconnaissance, patrol and strike missions. On the one hand, they are built from scratch along with their subsystems. On the other hand, in applique systems, existing weapon platforms such as infantry combat vehicles, combat jets, tanks and so forth, are modified to operate in tethered, semi-autonomous or in fully autonomous mode.

### *Role of Systems with Autonomy in Land Warfare*

The political and military objectives of warfighting continue to remain same, while land warfare and the technologies associated with it has undergone a massive change leading to the projection of power and coerce an adversary to come to terms with conditions tilted in favour of the superior power. This sort of strategy was evident during the Cold War when each side fielded their respective advanced weapon systems to awe the other and set the terms for negotiation. It is in that context that Marshal Nikolai Ogarkov (Chief of General Staff, Union of Soviet Socialist Republics, 1977–1984) talked about "military technological revolution" to appraise his leadership of the role of technology in future wars.[55] Part of his observation had an influence on America's role in Vietnam War (from 1961 onwards) in which US military used Ryan Firebee UAV and gathered necessary intelligence by flying around 3400 sorties.[56,57] In addition to that, the US Navy had also used guided glide bombs controlled by radio frequency communication link during the war.[58] By early 70s, a thought had already percolated into the psyche of the US strategic community that the RMA is the only way to sustain their superiority in future battlefields, where autonomous and intelligent weapon platforms will become a dominant trend. This is evident from the statement made by the US Army General William Westmoreland before Congress in 1970:

> "On the battlefield of the future, enemy forces will be located, tracked and targeted almost instantaneously through the use of data links, computer-assisted intelligence evaluation, and automated fire control. I am confident the American people expect this country to take full advantage of its

technology—to welcome and applaud the developments that will replace wherever possible the man with the machine."[55]

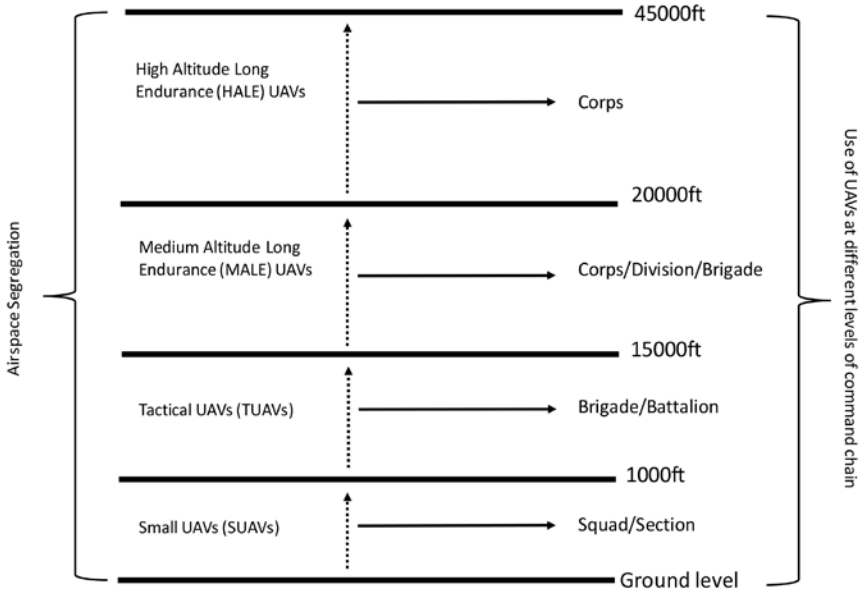
The intent was clear as the lessons learned from the use of glide bombs during Vietnam War paved the way for use of 'smart bombs' in the first Gulf War of 1991. Also, UAVs that proved to be an asset during 1970's were extensively used in Bosnia and Kosovo for reconnaissance missions during the third Balkan war of 1995. Prior to that, Israelis had already tasted success in the 1973 Yom Kippur war and 1982 Bekaa Valley battle, where they deployed UAVs to track down the enemy's air defences by releasing false radar signatures of an aircraft.[59] Interestingly, it was in early 1990's during the period of the first Gulf war when India's defence research and development agency began its ambitious program to develop an indigenous UAV named 'Nishant' based on radio frequency link technology.[60] However, it was only in 1996, that the Indian army acquired Searcher MK I UAVs from Israeli Aerospace Industries (IAI).[61] By then, UAVs had already become a tested platform among western militaries and infusion of machine intelligence was being conceived. The following figure lists the type of roles across which UAVs are used in military missions.

**Figure 12. Roles played by unmanned systems.**[60,63]

| | | | |
|---|---|---|---|
| Intelligence, Surveillance & Reconnaissance (ISR) ops | Target Location & Designation | Electronic Warfare | Counter Deception |
| Communication/Data Relay | Combat Search & Rescue | Weapon Strike | Nuclear Biological Chemical Reece |
| Battlefield Management | Mine Detection | Digital Mapping | Covert Sensor Insertion |
| Information Warfare | Border Patrol | Logistics | Explosive Ordnance Disposal |

The ambit of systems with autonomy in the context of land warfare includes UAVs, UGVs and Unmanned Ground Sensors (UGS). Roles assigned to these systems are divided across three levels namely, tactical, operational and strategic, and these are then distributed across battalions, brigades, divisions and corps respectively. For example, RQ-2 Pioneer UAVs with a flight ceiling of 15,000 ft were used for missions at the tactical level that includes reconnaissance, target acquisition and damage assessment missions, whereas RQ-5 Hunter UAVs with a flight ceiling of around 18,000 ft were used for reconnaissance and target acquisition tasks at division or corps level.[61] Similarly, micro UAVs (also known as Small UAVs [SUAVs]) are used by a squad or a section for reconnaissance missions. The following picture shows the use of unmanned aerial systems along with their flight ceiling across different levels of command.

**Figure 13. Air space segregation for deployment of UAVs.**[62]




***Factors Necessitating Deployment of Unmanned Systems***

The concept of autonomy and unmanned systems in defence are meant to ensure information dominance and force projection while ensuring low human casualty. Also, the objective is to have the real-time view of the battlefield and have a seamless flow of information across the command chain. However, there are other factors that necessitate the deployment of unmanned systems:

## Dull, Dirty and Dangerous

The real battlefield is all about dirt, dust and danger, where superior intelligence, well trained and equipped combatant ensures victory. However, there are instances in which troops are exposed to the harsh operating environment, repetitive as well as long working hours and dangerous missions that take a heavy toll on their psychological and physical health. This is evident from the fact that Indian troops deployed in the tropical jungles of North-east India and in the glacial heights of Siachen deal with the challenges posed by both weather and the enemy. Similarly, the US troops deployed in Iraq and Afghanistan face challenges both from hot weather and a vindictive enemy. During operation Global War on Terrorism (GWOT) in Afghanistan, the US forces sustained more causalities in Improvised Explosive Devices (IED) blasts rather than in actual combat. As a measure to address

such operational hazards, autonomous weapon platforms can be used to relieve their human counterparts from dull and dangerous tasks to some extent.[63] For example, TALON UGVs were used by US forces in Afghanistan for explosive ordnance disposal missions. UGVs and UAVs can be used for patrol and recce operations while unmanned sensors as part of ISR network can automatically sense, track and synchronise data with the Battlefield Management System (BMS) without human intervention.

### Deception

The advancement in air defence systems such as Patriot, S-300, and S-400 integrated with sophisticated radar technology has changed the equations on the battlefield. They pose a direct threat to the survivability of airborne assets such as combat jets, making war a costly affair. To counter this, a strategy was evolved to employ low-cost UAVs in Suppression of Enemy Air Defence operations.[64] There are instances such as 1973 Yom Kippur War and 1991 Persian Gulf War in which remotely piloted vehicles (RPVs) were used to stimulate enemy air defence radars in order to expose their locations.[65,66] Similarly, unmanned air launch flight vehicles such as Miniature Air-Launched Decoy can be used in SEAD operations.[67]

### Flexibility

Unmanned systems provide an opportunity and scope to enhance or modify any mission based on the requirement. For example, a UAV used in ISR operations can be used beyond its communication range through UAV relay network. Similarly, the flow of information into and across a command chain can be controlled through the selective use of ground-based sensors.

## AD in Land Warfare: Brief Overview

> The success of any major operation or campaign depends on the movement of one's force in the theatre. Without the ability to conduct large-scale movements on land, sea and in the air, operational warfare is essentially an empty concept
>
> —Dr. Milan Vego, Prof. Operations, UNWC[68]

### *The Concept*

In the history of land warfare, field armies have used a combination of different strategies and suitable weapon systems to deny their enemy access to or prevent its attempt to seize a territory of vital interest. This stratagem as a concept is referred to as A2/AD strategy.[69] The terminology 'A2/AD' was coined by the US based Centre for Strategic and Budgetary Assessment (CBSA) in its evaluation of the threats arising from the development of

strategic missiles and weapon systems by China and Russia. A2 as a concept represents the 'broad strategy' designed to prevent an adversary from entering into an area of operation through the use of different 'ways' and the available 'means' (available human and logistical resources). However, it is the concept behind the use of those available 'means to exploit different ways' which are referred to as AD strategy. In the context of the Indian army and in reference to its use in land warfare, the above concept is referred to as 'Defend and Control (DACO)' strategy.[70] Hence, in other words, A2 can be defined as the possible threats to the forces entering into an area of operation, whereas AD denotes the challenges faced by the forces operating within the area of operation.

The challenges arising out of the adversary's A2/AD stratagem may emanate from a range of actors either having the tacit or indirect support of the sponsoring state. They can either be non-state actors acting as a proxy element or a hybrid force bearing passive support of the enemy.[71] The non-state actors involve terrorist and insurgent groups such as militant groups operating in the Indian States to its North-East, terrorist groups operating in Jammu and Kashmir and Naxals in parts of Chhattisgarh and central India. Even though they lack capabilities to wage any large-scale offensive, they are capable of inflicting casualties on security forces. They generally operate in small units or in organised groups and use automatic weapons, IEDs and other low-tech weapons to engage with the security forces and deny them freedom of manoeuvre in the area of operation. On the other hand, in comparison with the non-state actors, hybrid forces are better equipped, well-trained and operate in a well-defined command and control setup capable of waging a full-scale asymmetrical warfare and is either independent or dependent upon the state that sponsors them. The examples include Viet Cong, Taliban, Hezbollah, Houthi Rebels, Kachin Independence Army and Border Action Teams of Pakistan army. Such forces bear potential to operate in structured formations. The type of weapons used by them may include man-portable air defense systems (MANPADS), automatic heavy machine guns, anti-aircraft guns and an armoured vehicle in small quantities, that may able to hold a terrain for a brief period of time. However, the use of AD strategy by the armed forces of an enemy state remains an obvious threat. The challenge posed by them would involve joint manoeuvres along with their air and naval arms to support land-based operations. In this case, the range of weapons used, such as UAVs with flight ceiling above 15,000 ft, long-range missiles, precision-guided munitions, air defence

batteries, tanks, combat vehicles, electronic and cyber weapons for jamming communication networks for AD operations can restrict the freedom of action within the area of operation.

***AD Weapon Systems***

Technological advances in navigation and precision guidance systems, progress in computing power and miniaturisation of processing systems have increased the complexity of the modern-day battlefield, providing an adversary with options to employ an effective strategy against an advancing force. The weapon platforms such as smart bombs, precision-guided munitions, automated aerial and land-based delivery platforms, using advanced technologies will pose a serious challenge to our forces operating in a high tempo area of operation. Some of these weapon platforms are briefly discussed below.

## Guided Missiles, Rockets and Artillery Munitions

These weapon systems have advanced targeting systems, both guided or unguided, and can be effectively employed against both static and dynamic targets. ATGMS such as NAG, AMOGHA-II can be operated both in semi-autonomous and remote-controlled modes that can be used against armoured columns of the adversary. On the other hand, possession of tactical missiles such as Iskandar, Lacrosse, BrahMos, Nasr with professional armies is destined to influence the terms of engagement on the battlefield.

## Precision Strike

The development of highly accurate navigation systems such as Global Positioning System (GPS), BeiDou, NaviC (IRNSS) has improved the accuracy of the cruise and ballistic missile systems. Not only that, the use of 'smart bombs' in Operation Linebacker and Operation Rolling Thunder during the Vietnam War and also during the 1991 Gulf War made it difficult for troops deployed by Viet Cong and Iraqis to hold the ground.[72]

## Advanced Air Defence Systems

It was in the 1983 Yom Kippur War that the Israeli Air Force raised its first UAV squadron and put them into active operation to activate the Egyptian Surface to Air Missile defence batteries to hunt them down later using its fighter jets. However, with the advent of advanced air defence systems such as S-400 (Triumph), the use of any such tactics can be effectively challenged. S-400 boasts of sophisticated radar that can identify, track and mow down unmanned air systems.

## Unmanned Combat Systems

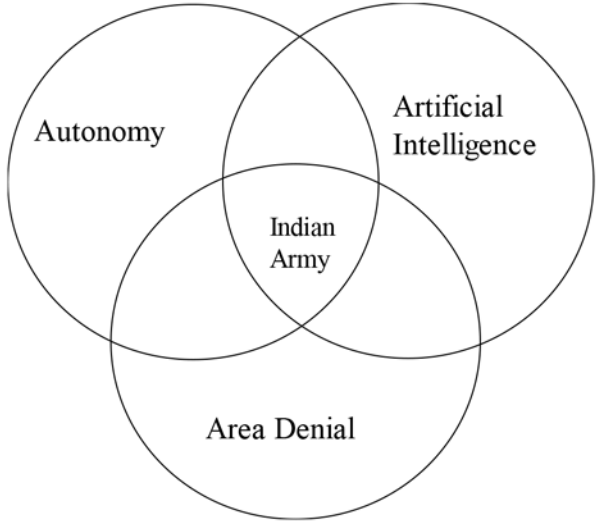
Apart from the initial task of ISR missions, unmanned combat platforms such as General Atomics MQ-9 Predator, IAI Hadoop, Talon and URAN-9 can be used for strike missions. These systems can also be used for disrupting Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) networks in the battlefield, thereby affecting AD operations.[73]

## Autonomy, AI & Army (3A): Model Analysis

The evolution in the realm of modern warfare since the two world wars and during the cold war period has made the battlefield more complex than it was ever before. The key to sustainment in these high tempo environments depends on the capability to sense, gather, collate, process and visualise the information of the events in real time, and deploy the required assets in the form of plug and play modules as part of the overall strategy. This has led to the requirement of a modern army that is well networked and integrated with other services to perform joint missions. This concluding chapter is important for two reasons. First, it discusses a model developed by integrating the concepts of Autonomy, AI and AD strategy. Second, it discusses the relevance of this model with respect to the Indian Army.

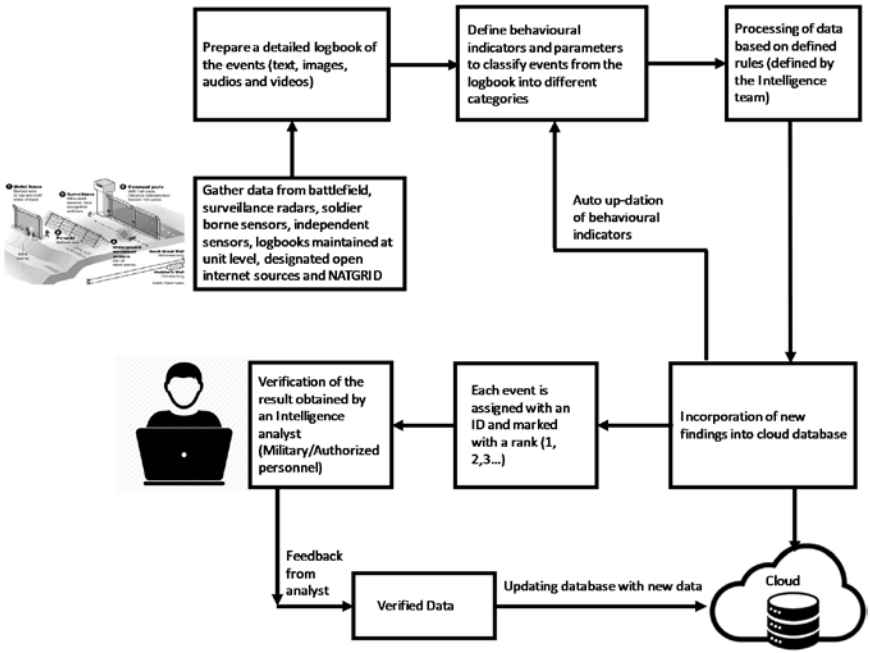
### *The 3A Model*

**Figure 14. The 3A model: the confluence of three concepts.**



The above picture shows the 3A conceptual model with the Indian Army as the user, residing at the intersection of the three concepts. The concept of autonomy involves the use of UAS, soldier-borne sensors and battlefield surveillance systems to drive the information into the army's command and control network with less human intervention.[74] However, it is through AI that the gathered information can be used to generate intelligence or initiate a command for autonomous weapon platforms to respond to a hostile situation along the border or in a conflict zone. The following figure illustrates a case of data collection and its analysis by an intelligence team. In this figure, the steps involving data collection, categorisation, analysis and updation of the database is a continuous process.

**Figure 15. AI-based predictive analysis of information to generate information.**[75]




The concept of AI can also help in automating certain aspects of a mission, such as the remote use of UGVs to respond to any infiltration attempt along the line of control while executing the task of border patrol. The incorporation of the third concept of AD requires the collaborative use of the first and second concept for any given task.

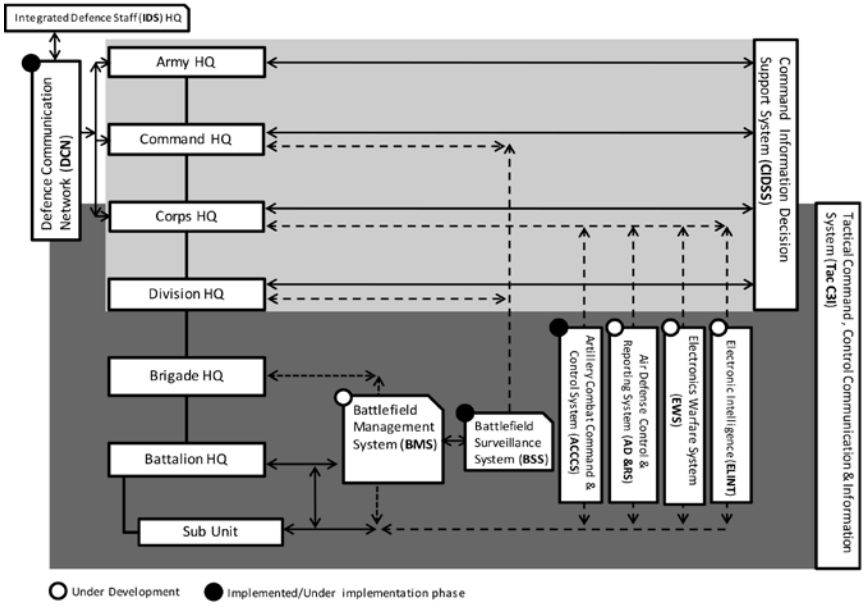
### *Components of 3A Model*

*The conceptualisation of the 3A model comprises of three components:*

- Command control and communication network.
- Cloud based database and AI applications.
- Unmanned systems and sensors (autonomy).

## Command Control and Communication (C3) Network

**Fig 15. Command & control channel for battlefield situation awareness for enhanced decision-making.[76]**




A robust command control and communication network is at the heart of the overall execution of the 3A model, without which each component is an isolated individual having capabilities, but no goal. This system consists of three stand-alone yet interconnected networks namely, Command Information Decision Support System (CIDSS), Tactical Command Control Communication and Information System (Tac C3I) and Defence Communication Network (DCN).[77] CIDSS forms a communication network from Divisional HQ to that of Army HQ (Integrated Defence Staff Headquarters (IHQ) (Army) of MoD) whereas TAC C3I will provide a robust communication network in a tactical battle area that can transmit audio, video and imagery data from a subunit to

that of corps HQ. The third, that is, DCN) will link (IHQ) with that of Corps HQ, Command HQ and Army HQ. The Tac C3I network composed of five subnetworks namely, ELINT, Electronic Warfare Systems (EWS), Air Defence Control and Reporting System (ADCRS), Artillery Combat Command and Communication System (ACCCS) and BMS. BMS is responsible to form a communication link between a subunit and Brigade HQ, including the Battalion HQ. It can be said that they are the fundamental communication networks that bring the concept of NCW to the tactical level. Also, ADCRS connects the army's air defence network with that of the air force.[78] The 3C network already have their defined architectures based on the cloud. It can access the central database and AI applications remotely over the cloud environment and can communicate with autonomous weapon platforms.

### Unmanned Systems and Sensors (Autonomy)

The last and an essential part of the overall model is autonomous weapon platforms and sensors. The application of the concept of autonomy depends on the effective use of autonomous systems and sensors at all levels of the battlefield These systems not only form an integral part of the NCW but also a medium to achieve information superiority over an area of operation. They are critical for the transmission of information from command and control network and develop an information grid. In case of the Indian army, unmanned systems are managed by its surveillance and target acquisition units. These units operate a mix of UAV systems that include IAI Heron, HAL Nishant, IAI Searcher Mk I and Mk II, Lakshya Remotely Piloted Vehicle (RPV) and UGVs such as DRDO Daksh. These autonomous systems are employed in various roles such as ISR missions, electronic warfare, signal intelligence, counter-deception and so forth. For instance, Heron and Searcher are medium altitude long endurance (MALE) UAVs capable of deployment at Corps, Division and Brigade level, while SUAV such as Netra, are suitable for deployment at squad or section level. Such systems can be deployed in our western and eastern frontier and if required, their operational range can be extended by using UAV relay network.[79] The following two figure shows the prioritisation of roles performed by UAVs in the army and their use across different formations.

**Figure 16. Prioritisation of roles of unmanned systems in army (ranked over scale 1-8).**[76]

| Roles | Priority Assigned |
|---|---|
| Reconnaissance | 1 |
| Target Location and Designation | 2 |
| Electronic Warfare | 3 |
| Signal Intelligence | 5 |
| Information Warfare | 2 |
| Counter Concealment and Deception | 4 |
| Communication/Data Relay | 6 |
| Weapon Strike | 8 |
| Battle field Damage Assessment | 4 |
| Mine Detection | 1 |
| Digital Mapping | 5 |
| Covert Sensor Insertion | 3 |
| Combat Search and Rescue | 7 |

**Figure 17. Types of UAVs used across different levels.**[80]

| Levels | Type of Unmanned Vehicle used | Roles |
|---|---|---|
| Corps | High Altitude Long endurance (HALE) UAVs | NBC Reece, ISR, EW, Combat |
| Division | Medium Altitude Long Endurance (MALE) UAVs | ISR, Armed Sorties |
| Brigade | Medium Altitude Long Endurance (MALE) UAVs | Reconnaissance, Surveillance and Target Acquisition, Explosive Ordnance Detection and Destruction |
| Battalion | Tactical UAVs (TUAVs), UGVs | |
| Squad | Small UAVs/ Micro UAVs, UGVs | ISR missions, Explosive Ordnance Detection and Destruction |

## Notes

1. Gary Chapman, "An introduction to the revolution in military affairs" (in XV Amaldi Conference on Problems in Global Security, Helsinki, Finland, September 25–27, 2003).
2. John R. Boyd, *Destruction and creation* (USA: US Army Command and General Staff College, 1987).
3. Sun Tzu, *The Art of War* (New York: Oxford University Press, 1963), p. 144.
4. Martin C. Libicki, *What is Information Warfare?* 1st ed. (Washington D.C.: National Defence University, 1995), p. 10.
5. Sharjeel Rizwan, "Revolution in Military Affairs," *Defence Journal*, September 2000, www.defencejournal.com/2000/sept/military.htm.
6. Gualtiero Piccinini, "The First Computational Theory of Mind and Brain: A Close Look at McCulloch And Pitts 'Logical Calculus of Ideas Immanent in Nervous Activity'," *Synthese: An International Journal for Epistemology, Methodology and Philosophy of Science* vol. 141, no. 2, 2004, pp. 175–215.
7. Alan Turing, "Computing Machinery and Intelligence," *Mind* vol. 59, no. 236, 1950, pp. 433–460.
8. Defence Science Board, "Report of the Defence Science Board Summer Study on Autonomy," (Office of the Under Secretary of Defence for Acquisition, Technology and Logistics, June 2016), p. 5. https://www.hsdl.org/?view&did=794641
9. John Launchbury, "A DARPA Perspective on Artificial Intelligence," YouTube video, (February 15, 2015). https://youtu.be/-O01G3tSYpU
10. Paul Mozur, "Google's AlphaGo Defeats Chinese Go Master in Win for A.I.," *New York Times,* https://www.nytimes.com/2017/05/23/business/google-deepmind-alphago-go-champion-defeat.html, accessed on August 07, 2017.
11. Michael Nielsen, *Neural Networks and Deep Learning,* 1st ed. (United States: Determination Press, 2015), Chapter 1.
12. Ibid., Chapter 2
13. M. Corporation, "Tay Tweets,"https://twitter.com/TayandYou, accessed on August 07, 2015.
14. Sarah Perez and TechCrunch, "Microsoft Silences its New A.I. Bot Tay, after Twitter Users Teach it Racism [Updated],"TechCrunch, https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/, accessed on August 07, 2017.
15. Stephan De Spiegeleire, Matthijs Maas and Tim Sweijs, *Artificial Intelligence and The Future of Defence,* 1st ed. (Hague, Netherlands: The Hague Centre of Strategic Studies, 2017), pp.12–13.
16. Dustin A. Lewis, Gabriella Blum and Naz K. Modirzadeh, "War-Algorithm Accountability," (August 31, 2016). https://ssrn.com/abstract=2832734
17. Spiegeleire, n. 15, p. 30.
18. Ministry of Defence, Bharat Dynamics Limited (BDL) [Brochure], Hyderabad, BDL.
19. Machine Intelligence Research Institute (MIRI), (2013) What is AGI? - Machine Intelligence Research Institute. Retrieved 9 Aug 2017, from: https://intelligence.org/2013/08/11/what-is-agi/.
20. Chrisantha Fernando et al, PathNet: Evolution Channels Gradient Descent in Super Neural Networks, https://arxiv.org/abs/1701.08734
21. Spiegeleire, n. 15, p. 40.
22. William Bryk, "Artificial Superintelligence: The Coming Revolution," Harvard Science Review, https://harvardsciencereview.com/2015/12/04/artificial-superintelligence-the-coming-revolution-2/, accessed on August 10, 2017.
23. Spiegeleire, n. 15, pp. 13–18.
24. BS Web Team, "All you need to know about NATGRID and its new CEO Ashok Patnaik,"

*Business Standard*, http://www.business-standard.com/article/current-affairs/all-you-need-to-know-about-natgrid-and-its-new-ceo-ashok-patnaik-116071400134_1.html, accessed on August 10, 2017.
25. Digital Signal Processing Group (AGH University of Science and Technology), "Artificial Intelligence and Neural Networks," http://www.dsp.agh.edu.pl/_media/en:dydaktyka:artificial_intelligence_and_neural_networks.pdf, accessed on August 10, 2017.
26. Vijipriya D. Jeyamani, Jammi Ashok, and S. Suppiah, "A Review of Significance of Sub Fields in Artificial Intelligence," *International Journal of Latest Trends in Engineering and Technology* vol. 6, no. 3, 2016, pp. 542–546.
27. Robin Sandhu, "Applications of Natural Language Processing," *Lifewire*, https://www.lifewire.com/applications-of-natural-language-processing-technology-2495544, accessed on August 13, 2017.
28. Winfred Phillips, "Introduction to Natural Language Processing," http://www.mind.ilstu.edu/curriculum/protothinker/natural_language_processing.php, accessed on August 13, 2017.
29. Dr. Boyan Onyshkevych, "Deep Exploration and Filtering of Text (DEFT)," *DARPA*, https://www.darpa.mil/program/deep-exploration-and-filtering-of-text, accessed on August 13, 2017.
30. Derrick Harris, "DARPA is working on its own deep-learning project for natural-language processing," *Gigaom* https://gigaom.com/2014/05/02/darpa-is-working-on-its-own-deep-learning-project-for-natural-language-processing/, accessed on August 13, 2017.
31. Mohammad Al-Raba bah and Abdusamad Al-Marghilani, "Artificial Intelligence Technique for Speech Recognition Based on Neural Networks," *Root to Fruit: Artificial Intelligence Technique for Speech Recognition Based on Neural Networks* vol. 7, no. 3, 2015, pp. 331–336.
32. Reed, *The Design and Requirements Evolution of a Speech Recogniton Technology for Tactical Applications and Environments [pdf]* (New Jersey: US Army RDECOM CERDEC, n.d).
33. ARL Public Affairs and Joyce Brayboy, "Computers Harness Language Translation—US Army RDECOM—Medium," *Medium*, https://medium.com/@RDECOM/computers-harness-language-translation-c250adb765b8, accessed on August 14, 2017.
34. Bradley G. Boone, et al., "New Directions in Missile Guidance," *John Hopkins APL Technical Digest* vol. 11, no. 2, 1990, pp. 28–35
35. Army Capabilities Integration Centre, "The US Army Robotics and Autonomous Systems Strategy," Army Capabiloties Integration Centre, 2017. http://www.arcic.army.mil/App_Documents/RAS_Strategy.pdf
36. Raj Shukla, "Military Frontiers of Global War on Terror: Some Lessons," CLAWS, http://www.claws.in/images/journals_doc/1254626087_RajShukla.pdf
37. Carl Prine, "Robots Poised to Take Over Wide Range of Military Jobs," *The San Diego Union-Tribune*, http://www.sandiegouniontribune.com/military/sd-me-robots-military-20170130-story.html, accessed on August 15, 2017.
38. Parliamentary Office of Science and Technology, Automation in Military Operations: Postnote, No. 511, http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0511#fullreport
39. Psibernatix, "Defense—Psibernetix Inc.," http://www.psibernetix.com/projects/defense/, accessed on August 15, 2016.
40. "Collaborative robots, or COBOTS as they are known to the cognoscenti, are robots that are designed to operate collaboratively with humans. They are designed to be safe around people, either by force limiting to avoid injury if they touch, by sensors that prevent touching or by a combination of both. The ISO standards that govern employment of COBOTS are ISO 15066, 10218 part 1 and part 2."
41. Spiegeleire, n. 15, pp. 40–42

42. Ciro Donalek, "Supervised and Unsupervised Learning," *Caltech Astronomy, 2011*. http://www.astro.caltech.edu/~george/aybi199/Donalek_Classif.pdf
43. E. W. Naef, "NATO: The Revolution in Military Affairs," *IWS*, http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html#1, accessed on August 19, 2017.
44. Martin Van Creveld, *Technology and War: From 2000 BC to the Present*, 1st edition (Toronto, Canada: Maxwell Macmillan International, 1991), pp.1–23.
45. Alexander Lychagin, "Что такое телетанк?," *Odintsovo*, http://www.odintsovo.info/news/?id=1683, accessed on August 17, 2017.
46. "Back to the Drawing Board—The Goliath Tracked Mine," *Military History Monthly*, https://www.military-history.org/articles/back-to-the-drawing-board.htm, accessed on August 17, 2012.
47. Department of Defense (US), "Network Centric Warfare," 2001. http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf
48. Lora G. Weiss, "Autonomous Robots in the Fog of War," *IEEE Spectrum*, 2011. http://spectrum.ieee.org/robotics/military-robots/autonomous-robots-in-the-fog-of-war, accessed on August 18, 2017.
49. *Kris Osborn,* "Marines Test Tethered Unmanned Vehicle," *Defense Tech, 2014*. https://www.defensetech.org/2014/09/25/marines-test-tethered-unmanned-vehicle/, accessed on August 18, 2017.
50. SDR Tactical, "HD2 Tactical Treaded Robot with Arm," *SDR Tactical*, http://sdrtactical.com/HD2Arm-Mastiff/, accessed on August 18, 2017.
51. Ryan O'Hare, "Iraqi Army Fight ISIS using New Remote-Controlled Robotic Tanks," *Mail Online*, 2016, http://www.dailymail.co.uk/sciencetech/article-3754832/Meet-Alrobot-remote-controlled-robotic-tank-used-Iraqi-army-fight-ISIS.html, accessed on August 18, 2017.
52. Kristin Houser, "The Marines' Latest Weapon Is a Remote-Controlled Robot With a Machine Gun," *Futurism*, https://futurism.com/the-marines-latest-weapon-is-a-remote-controlled-robot-with-a-machine-gun/, accessed on August 18, 2017.
53. Maryland Robotics Center, "Semi-Autonomous Systems Laboratory," http://robotics.umd.edu/labs/semi-autonomous-systems-laboratory, https://futurism.com/the-marines-latest-weapon-is-a-remote-controlled-robot-with-a-machine-gun/, accessed on August 18, 2017.
54. "Teleoperation," Department of Computing Engineering, 2011. https://www8.cs.umu.se/kurser/5DV053/VT11/utdelat/Lectures/Teleoperation.pdf
55. Chapman, n. 1.
56. Thomas P. Erhard, "Air Force UAVs: The Secret History," Defence Technical Information Centre (DTIC), 2010. http://www.dtic.mil/dtic/tr/fulltext/u2/a525674.pdf
57. National Research Council, et al., *Autonomous Vehicles in Support of Naval Operations* 1st edition (Washington D.C: National Academies Press, 2005), p. 82.
58. Carlo Kopp, "Milestones: Smart bombs in Vietnam," *Defence Today*, vol. 7, no. 6, 2009, pp. 42–44.
59. Lt Col Richard P. Schwing, *Unmanned Aerial Vehicles—A Revolutionary Tool in War and Peace* (Carlisle Barracks, Pennsylvania, United States: US Army War College, 2007).
60. Manu Pubby, "DRDO's Two-Decade-Old Nishant UAV Programme Crashes; Indian Army cancels further orders," *The Economic Times*, November 17, 2015, http://economictimes.indiatimes.com/news/defence/drdos-two-decade-old-nishant-uav-programme-crashes-indian-army-cancels-further-orders/articleshow/49809095.cms, accessed on August 19, 2017.
61. Gp. Capt. Joseph Noronha, "Flying High: The Bright Future of India's Military UAVs," *Indian Defence Review*, 2015. http://www.indiandefencereview.com/news/flying-high-the-bright-future-of-indias-military-uavs/, accessed on August 19, 2017.
62. Centre for Land Warfare Studies, "Future of Unmanned Systems," 2012, New Delhi, India

63. Jurgen Altmann and Frank Sauer, "Autonomous Weapon Systems and Strategic Stability," *Survival: Global Politics and Strategy*, vol. 59, no. 5, 2017, pp. 117–142.
64. Robert E. Suminsby, *Unmanned Combat Air Vehicles for Suppression of Enemy Air Defences* (Maxwell Air Force Base, Alabama: Air War College, Air University, 2018), http://www.dtic.mil/dtic/tr/fulltext/u2/a420687.pdf, accessed on February 21, 2018.
65. Z. C. Zhao, X. S. Wang and S. P Xiao, "Cooperative Deception Jamming Against Radar Network Using a Team of UAVs," (paper presented at the IET International Conference, Guilin, China, April 20–22, 2009, 603).
66. Air Israeli Force, *"The First UAV Squadron," Last modified 2018.* http://www.iaf.org.il/4968-33518-en/IAF.aspx, accessed on February 21, 2018.
"The Chukar's main aim was to draw enemy antiaircraft fire, making it easier for combat planes to locate and destroy the missile batteries. The Chukar received its baptism by fire during the Yom Kippur War. During the Yom Kippur War, the Chukar was used to mislead enemy antiaircraft batteries. On 7th October 1973, the Chukars were launched in the north for the first time, towards the Golan Heights, and fooled the Syrians into thinking that a massive combat plane strike had begun against their AA positions. During the war 23 of the Chukars were launched, 18 returned and 5 fell. Each group of between two and four of the UAVs drew 20–25 Egyptian rockets, demonstrating the effectiveness of the system. Throughout the war, more Chukars arrived from the US. On the southern front a Firebee squadron was deployed on the frontlines but following an Egyptian MiG-17 attack they returned to an airbase. The Firebees operated intensively throughout the 12 days of fighting, carrying out 19 flights during which 10 Firebees were lost. At the end of the war, only 2 Firebees remained in the squadron".
67. Airforce Technology, "Miniature Air Launched Decoy (MALD) Flight Vehicle," *Airforce Technology,* http://www.airforce-technology.com/projects/miniature-air-launched-decoy-mald-flight-vehicle/, accessed on February 21, 2018.
68. Major Christopher J. McCarthy (US Air Force), "Chinese Anti Access/Area Denial: The Evolution of Warfare in the Western Pacific," Joint Military Operations Department, USNWC, US, 2006, p.3.
69. Andrew Krepinevich, Barry Watts and Robert Work, "Meeting the Anti Access Area Denial Challenge," CSBA, Washington DC, US, 2003, p. 4.
70. Brig. Narendra Kumar, Senior Fellow, CLAWS, in conversation with author, May 2017.
71. John Gordon IV and John Matsumura, "The Army's Role in Overcoming Anti-Access and Area Denial Challenges," RAND Corporation, Arroyo Centre, US, 2013, p. 5.
72. Patrick Coffey, *American Arsenal*, 1st edition (New York: Oxford University Press, 2014), p. 273.
73. Gordon IV, n. 72, p. 12.
74. Nath Chandrika and Christie Lorna, "Automation in Military Operations of UK," POST notes, no. 511, pp. 1–5, at http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0511
75. In consultation with CLAWS faculty, senior fellow, July 2017.
76. CLAWS Faculties, Senior Fellows, in conversation with Author, June-July 2017.
77. Maj General PK Chakravorty (Retd), "State of Modernisation of the Indian Army," *India Strategic*, 2014, http://www.indiastrategic.in/topstories3160_State_of_Modernisation_of_Indian_Army.htm, accessed on August 21, 2017.
78. Lt Gen Prakash Katoch, "Network Centric Warfare," *Indian Defence Review*, 2013, http://www.indiandefencereview.com/news/network-centric-warfare/, accessed on August 21, 2017.
79. Boyang Li, et al., "Development and Testing of a Two-UAV Communication Relay System," *Sensors,* vol. 16, no. 10, 2016, p. 1696, Hong Kong China.
80. Centre for Land Warfare Studies, n. 63.