

PREDICTING ADVERSARY'S PSYCHE AND INTENT USING ARTIFICIAL INTELLIGENCE

SHAURYA DHAKATE

In the 21st century, the scenarios on the battlefield have become very dynamic. They tend to change in accordance with the leadership's aims on both sides. The intentions and the feelings of the troops are not very fast changing, they remain more or less the same throughout the course of a conflict. So, why do we observe sudden shifts in situations during wartime? The troops' actions play a significant role in defining the state of international relations. To get accurate information about the adversary's headquarters, latest capabilities and plans, modern tactics of espionage tools and redesigned intelligence agencies saw the light of the day a century back. In present-day scenario, most of the work done by 'foot soldiers' in intelligence can be performed by a single person on a desk or even by an automated programme. Personal IT devices in the hands of every citizen can act as an eye, which observes the person rather than the world.

Today is the era of big data, when we have the capacity to gather massive amounts of information. Application of Artificial Intelligence (AI) has been successfully utilised in a variety of industries, such as technology, banking, marketing, and entertainment. The advent of AI and increased usage of IT has led to what is called "Surveillance Capitalism". Shoshana Zuboff, an American author, Harvard professor and social

Mr. **Shaurya Dhakate** is an independent researcher. His principal research areas include information warfare, airpower and national security.

The common notion across citizens is that we are the users of technology, but in reality, we are just instruments for technology to gain more data. The price, type of product we seek and the searches we do are recorded in order to analyse patterns of consumer's thinking.

psychologist writes, "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Even though some of these collected data are applied to product and service enhancement, the rest are acknowledged as a proprietary behavioural surplus, which are fed into advanced engineering processes also known as 'machine intelligence', and further fabricated into prediction products that foretell what you will do now, soon, in the close and distant future. Finally, these prediction products are bartered in a new kind of marketplace called behavioural futures markets".¹

Our everyday interactions with the Social Networking Sites (SNS) play a mammoth role in helping organisations in conducting Behavioural Market Research (BMR) by continuously monitoring our IT devices. The common notion across citizens is that we are the users of technology, but in reality, we are just instruments for technology to gain more data. The price, type of product we seek and the searches we do are recorded in order to analyse patterns of consumer's thinking. These strategies not only help in simple marketing of products and services, but also in research.

Data is a gold mine in the current times; getting the right data might be the most valuable asset in cyber warfare between nations. Sharon Weinberger, in one of her speeches, talked about a defence consultant who went to Uzbekistan. The consultant's role there was of assistance in selling technology that the Uzbek government could use to spy on its own citizens. He eventually shared the marketing material he had presented to the Uzbek government. One glossy brochure featured technology that could not only intercept phone calls, but also identify the caller and the receiver, based on

1. Shoshana Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", *Public Affairs*; 1st edition (January 15, 2019). Accessed on May 19, 2021.

the unique voiceprint, regardless of what phone number they were using, and then identify their precise geographic location. The consultant was a person who had been involved with the arms trade for years. He had partnered with legitimate Western companies to help sell their weapons abroad. But he wasn't concerned about marketing this sort of technology. "For him, it was just the next step in the arms trade. And it was even easier than, say, selling weapons to Iraq, because it did not require an export license from the US State Department, as most arms sales would. It turns out that these sort of tools of surveillance are nearly completely unregulated, because, as of today, they are not defined as weapons".²

For the working of AI and prediction of behaviour and emotions, not only programming and machine learning are required to develop the technology, various other fields of study and research must also come into play.

For the working of AI and prediction of behaviour and emotions, not only programming and machine learning are required to develop the technology, various other fields of study and research must also come into play. For instance, if you want a software to predict behaviour of one particular person or a society, then it must first learn how people from different areas and cultures respond to certain situations. But even before grasping that, it must understand human psychology in general. Marketing, today, involves understanding the functioning of the brain, and more specifically, how to make people want and like something in order to create an addiction to it. There is a term called "Diderot effect", the effect of which is that getting a new possession often causes an ever increasing spiral of consumption that leads to keep on wanting more and more. We can spot this pattern everywhere. It creates a chain reaction and many human behaviours follow this cycle. This is not only useful in marketing and business research but also for prediction of mass opinion of any particular issue. The public opinion

2. Sharon Weinberger, in her TED speech "Inside the massive (and unregulated) world of surveillance tech, 28", TED Talk, December 28, 2020.

during war plays a huge role in deciding the outcome, since it determines the amount of pressure to be applied on the government.

The Geometric Algorithms for Modelling, Motion, and Animation (GAMMA) group at the University of Maryland at College Park, works on many different research problems, including multi-modal behaviour learning using Artificial Intelligence, research into robot navigation and autonomous vehicles, and physically-based simulation. Specifically, one of the most intriguing features of their present research is their work on “socially-intelligent robots”. The most thought-provoking research applications of socially-intelligent robots are their capabilities to read and comprehend body language. Research conducted by the GAMMA lab is aiming to study and develop AI systems that can detect emotions based on gait (a person’s manner of walking). The lab puts into use the selected facial expressions with body motion as a way to improve prediction of humans’ emotional states. According to the lab researchers at Maryland, in the case of gaits, walking style of people is not something that can be simply manipulated. Recognizing people based on their way of walking and moving using AI systems has already been widely publicised and shown to have a certain degree of accuracy. Gait detection and proper identification of walking trajectories when combined with the subject’s facial expressions in a given controlled or uncontrolled pedestrian setting can predict their future walking behaviours and present emotional states. The research participants believe that socially intelligent programs can be successfully applied in many different applications, such as those involved in developing automated methods for perceiving human emotions in therapy, rehabilitation, anomaly detection and surveillance, understanding audiences, character generation for animation and movies, etc.³

The organisations benefit from the collection and amalgamation of vast amounts of data about billions of people, dead or alive, by processing it and creating automated programmes and software that collect more data. These can be used for a variety of things, including warfare.

3. Ron Schmelzer, “Can AI detect your emotion just by how you walk?”, *Cognitive World, Forbes*, March 29, 2020.

CORE ANALYSIS

With all the developments in technology, two important questions must be addressed: (1) How will role of artificial intelligence impact future conflicts? (2) How are countries developing AI software and weaponry for future warfare? The following paragraphs seek to undertake this exploration in the hope that strategic researchers and students, both in India and elsewhere, can gain a better understanding of the role and importance of new technologies (particularly AI) in future conflicts.

International Arena

Artificial intelligence in the contemporary times is not just a consumer—or business and consumer-centric-focused technology. Indeed, companies are using AI to automate various tasks, while consumers are using AI to simplify their daily routines. But governments and particularly militaries also have a significant interest in the speed and scale offered by AI. Nation states have already started using artificial intelligence to monitor activities of their own citizens. The UK's Ministry of Defence (MoD) recently revealed that they will use AI to make decisions related to national security and warfare. The MoD's Defence and Security Accelerator (DASA) has announced the initial injection of £4 million in funding for new projects exploring how to use AI in the context of the British Navy.⁴ DASA is planning to effect enhanced usage of AI and machine learning-based technology to revolutionise the way decisions are carried out by military equipment by processing millions of packets of intelligence and data.

Like Britain, other countries too are granting funds to agencies dedicated to research and development (R&D) of AI in response to the fact that the world's leading military powers have incorporated the use of machine intelligence and automation into their battlefields. While not many companies can build missiles or aircraft, it does not take a lot of capital

4. Simon Chandler, "How Artificial Intelligence will make Decisions in Tomorrow's Wars", *AI, Forbes*, January 20, 2020, at <https://www.forbes.com/sites/simonchandler/2020/01/20/how-artificial-intelligence-will-make-decisions-in-tomorrows-wars/?sh=2acbd8b04e01>. Accessed on May 19, 2021.

and heavy machinery to create a software that can hack into someone's smartphone. The Pentagon and CIA have tried to build technologies that can track suspected terrorists around the globe. The Pentagon has invested in something called smart dust, tiny microensors the size of specks of dust that can be sprinkled on people without their knowing it, and then use this to track their location. The Pentagon, via its venture capital firm, invested in a beauty products company once highlighted in Oprah Magazine to build a system that could surreptitiously collect DNA just by swiping across the skin. In 2008, the Pentagon had secretive databases of DNA from terrorists. It had about 80,000 samples. Indeed, the private company AncestryDNA today has DNA samples from about almost 15 million people. 23andMe, which is the second-largest genealogical database, has samples from over 10 million people. In the United States and China, AI researchers are working on using DNA samples to build images of people's faces. So, if we pair DNA with facial recognition technology, we can create a very powerful surveillance system capable of tracking individuals or entire ethnic groups.⁵ The Pentagon issued a memo to all its service members specifically urging them not to use those commercial DNA kits over which there were concerns that information could be used to track them or their family members. And yet, despite the Pentagon raising concerns about the technology, little effort has been made to rein in this market.

When it comes to the use of Artificial Intelligence, the Pentagon's research arm approved a grant of US\$ 1 million for a contract to build an AI tool for the purpose of decoding and predicting the emotions of allies and enemies. The plan is to get the AI app to advise military leaders on major military decisions. The Defence Advanced Research Projects Agency's (DARPA) backing for the project serves as a competition to get ahead in the race to use AI to predict emotions. The DARPA project is named PRIDE (Prediction and Recognition of Intent, Decision and Emotion) with the objective to create an AI system for understanding and predicting reactions of a group or an individual, to provide guidance on further course of action.

5. Weinberger, n. 2.

In the Farrington, London, offices of Element Human, its 36 year old founder, Matt Celuszak, asserts grand claims that such emotion recognition is about to produce a substantive change in how people live their lives and how humanity is evolving. His company works with clients “to sharpen the quality of their video ads to hit emotional triggers of their audiences by showing them to a small audience and having algorithms look for signs of emotion, whether that’s slight amusement or terror”.⁶ Until now, the company has primarily operated in secret, while testing the technology with various media houses.

PAF’S CENTAIC AND AI IN DRONE TECHNOLOGY

After Pakistan Air Force’s (PAF) Operation Swift Retort in February 2019, the Pakistani leadership recognised the importance of using air power as the main element for utilisation of Artificial Intelligence/Machine Intelligence and Cognitive Electronic Warfare (CEW). Pakistani military is now fully committed to the new technology of AI and has established the Centre for Artificial Intelligence and Computing (CENTAIC) at its Air University for taking this initiative to its logical conclusion. “CENTAIC will allow PAF to develop and empower sensor fusion technology, which combines sensory data from multiple sources such as radars, LIDARS and cameras to form a single model having the least uncertainty as it balances the strengths of different sensors”.⁷

The full spectrum of the scope of CENTAIC’s mandate has not been made transparent for those not involved in the project, but it is well known that the project’s main elements would be research on AI, big data, deep learning, machine learning, predictive analytics and Natural Language Processing (NLP). The various elements given above are valid not just for future of air warfare like RPA technology but also for applications—notably drone

6. Thomas Brewster, “DARPA Pays \$1 Million for an AI App that can Predict an Enemy’s Emotions”, *Cybersecurity, Forbes*, July 15, 2020, at <https://www.forbes.com/sites/thomasbrewster/2020/07/15/the-pentagons-1-million-question-can-ai-predict-an-enemys-emotions/?sh=793575ac32b4>. Accessed on May 19, 2021.

7. PtProfit, “PAF Establishes Centre for Artificial Intelligence”, August 31, 2020, <https://profit.pakistantoday.com.pk/2020/08/31/paf-establishes-center-for-artificial-intelligence/>

Jammers, drone radars and power lasers can be a huge leap forward in providing a new blanket of defence to Indian military establishments. These technologies are already in active use with several militaries across the globe. With AI being incorporated into such devices, we can automate the responses that it needs to take when a blip is seen on the radar.

development and research towards its next-generation fighter aircraft (NGFA).

With the novel drone threat, air assets are now more threatened, even when stored in hangars and blast pens anywhere in the nation. The drones, being a few feet in diameter have no limit for infiltration and can be operated by a single person in a vehicle just a few hundred metres away from an airfield perimeter. 'Swarm of Drones' may be a new concept in the Indian subcontinent but these have been in successful application in countries like Israel and Syria for years. During wartime, India may witness these swarms

racing towards military establishments to degrade its airpower in forward bases. With these drones capable of breaking multi-layered cemented roof tops with the help of explosives, we must not overlook and deny the scenario of a day when one drone with explosives causes a chain-reaction of blasts in a squadron hangar. CENTAIC may be looking into these broad possibilities to incorporate AI into drone technology, where the accuracy of attack can grow exponentially with minor scope of error, high level of deniability and very low levels of risk. Jammers, drone radars and power lasers can be a huge leap forward in providing a new blanket of defence to Indian military establishments. These technologies are already in active use with several militaries across the globe. With AI being incorporated into such devices, we can automate the responses that it needs to take when a blip is seen on the radar.

China is investing heavily in AI technology in an effort to become the leader across the world in exploitation of AI technology. The PLA firmly believes that AI is now a potent tool for countering the quantitative and qualitative superiority possessed by the Western powers, specifically the

NATO alliance led by the US. Consequently, the Chinese leadership has made this a key result area for the modernisation of its military arsenal with AI embedded enablers in a short span of time. The progress made in fields like AI enabled aircraft, drones at sea, autonomous submarines and cruise missile technology is being carried out at a rapid pace.

The development of AI based applications for the battlefields is very fast paced. From automating missiles to predicting and deciding the best decision, AI will be able to do most of the tasks in future warfare. The F-86E Sabre was one of the first USAF fighter aircraft to feature a small radar to aid the pilot with aerial gunnery. Determining the range to an enemy target had always been a challenging prerequisite to a successful gunshot.⁸ Today, machines can outperform humans. An AI algorithm has beaten a human fighter pilot in a virtual dogfight.⁹ Heron defeated a human fighter pilot, who was seated in a simulator and wearing a virtual reality helmet, by a score of five rounds to zero.

Last but not the least, “Russian weapons manufacturer Kalashnikov is working on an automated gun system that uses artificial intelligence to make shoot/no shoot decisions. But exactly how this AI or any other decides who is and is not a combatant is at the centre of a fierce argument over allowing autonomous weapons on battlefields filled with both soldiers and civilians. A module in it makes use of neural network technologies that enable it to identify targets and make decisions. A significant part of neural networking technology is the ability to learn lessons from past mistakes. Neural networks are computer programs that learn, much like the way animal brains do, from

Exactly how this AI or any other decides who is and is not a combatant is at the centre of a fierce argument over allowing autonomous weapons on battlefields filled with both soldiers and civilians.

8. NATO Defence College, “Automation in Air Warfare: Unpacking the Challenges of Human-Machine Interaction,” NATO Defense College (2019), at <http://www.jstor.com/stable/resrep19966.10>. Accessed on May 22, 2021.

9. Patrick Tucker, “An AI Just Beat a Human F-16 Pilot In a Dogfight—Again”, *Science & Tech, Defence One*, August 20, 2020, at <https://www.defenseone.com/technology/2020/08/ai-just-beat-human-f-16-pilot-dogfight-again/167872/>. Accessed on May 23, 2021.

example and then use that learning to make effective decisions in the future. A battlefield robot during a chaotic combat, for example, may store images of both soldiers, guerrillas, and unarmed civilians in an onboard database. Once its onboard cameras detect and recognise a human being, the neural network compares the person it is seeing to the features fed in the database. "If it has a firearm or uniform or logo used by enemy troops, it would open fire. Ideally, if it saw no weapon or arms at all, it would judge the target a civilian and would not open fire".¹⁰ The problem with example-based learning in warfare is that in war mistakes are permanent and irreversible, and a neural network may be unable to apply learnt lessons. If the robot misjudges a rocket launcher as a broomstick and does not fire, the rocket launcher will blow it up.

India's Development and Application of AI for Warfare

Before proceeding to address the development of artificial intelligence in India, it is necessary to separate the concept of artificial intelligence in warfare into two categories: (1) Use of AI as hard power; and (2) Use of AI as soft power. The former seeks to modify the current military equipment and indigenously develop new ones with the inclusion of machine learning and software-controlled systems. The latter, meanwhile, is more suited for espionage, influencing and controlling behaviours during high tensions.

India is already looking to upgrade its defence inventory with modern technologies such as Artificial Intelligence and Augmented Reality (AR), which are likely to become the lifeline of modern military. The Ministry of Defence has initiated the process of preparing Indian defence forces for use of AI. To study the whole range of issues on the implications of this employment on national security and defence needs, a multi-stakeholder task force on Strategic Implementation of Artificial Intelligence for National Security and Defence was constituted in February 2018. The task force was represented by delegates from the government, defence services, academia, industry professionals, Defence

10. Kile Mizokami, "Kalashnikov Will Make an A.I.-Powered Killer Robot", *Popular Mechanics*, July 19, 2017, at <https://www.popularmechanics.com/military/weapons/news/a27393/kalashnikov-to-make-ai-directed-machine-guns/>. Accessed on May 21, 2021.

Research and Development Organisation (DRDO), National Cyber Security Coordinator (NCSC), Defence Public Sector Undertakings (DPSUs), Indian Space Research Organisation (ISRO) and Bhabha Atomic Research Centre (BARC). The task force studied and analysed research and innovation in Artificial Intelligence and how it can be adopted in the Indian defence sector. “The DPSUs (Defence Public Sector Undertakings) and ordnance factories have been instructed to develop AI-enabled products. A project has been authorized to the Centre for Artificial Intelligence and Robotics (CAIR), a DRDO based laboratory”.¹¹ The project given to CAIR aims at enhancing intelligence collation with the goal of strengthening analysis capabilities of the Indian armed forces. The project has a cost of Rs 73.9 crore. “Energy Harvesting Based Infrared Sensor Network for Automated Human Intrusion Detection” (EYESIRa) is another project that has been sanctioned for a budget of approximately Rs 1.8 crore. AI and machine learning tools will become useful for the armed forces in the fields of decision support, sensor data analysis, predictive maintenance, situational awareness, accurate data extraction, security, etc. Niti Aayog’s 2018 document entitled ‘National Strategy for Artificial Intelligence’ emphasises the adoption of AI in India and the major challenges that it could face.

It is to be noted that the NITI Aayog document majorly emphasises upon the future engagement of artificial intelligence in five sectors: healthcare, agriculture, education, smart cities and infrastructure and last but not the least, smart mobility and transportation. “Furthermore, it proposes that for an accelerated adoption of an extremely collaborative technology like AI, the government has to play the critical part of a catalyst in supporting partnerships, providing infrastructure access, fostering innovation through research and generating the demand by seeking solutions for addressing numerous governmental needs”.¹² We must agree that putting AI into use in these sectors can benefit the nation and its future, we must not forget that the armed forces require the cutting-edge technologies to be a cut above the rest.

11. PIB Delhi, Artificial Intelligence, January 2, 2019, at <https://pib.gov.in/PressReleasePage.aspx?PRID=1558146>. Accessed on May 30, 2021.

12. NITI Aayog, “National Strategy for Artificial Intelligence”, Discussion Paper, June 2018, at https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf. Accessed on May 30, 2021.

India, with its enormous talent pool and potential, must get into the act or else we might be constrained to fight a battle in a preconceived manner while our adversaries attack us through different domains using the disruptive power of AI. The last generation was that of RMA (Revolution in Military Affairs). With the arrival of Artificial Intelligence, AR/VR, Robotics, Big Data analytics, cyber technology and other disruptive technologies, we have entered an era of Disruption in Military Affairs (DMA). Central to all these technologies is AI and Machine Learning. Familiarity of AI is today better with the youth, but, they have little knowledge about modern warfare, battlefields and weapons. Soldiers possess extensive knowledge about the latter but have little knowledge of AI. Building AI into a tool of war requires a great volume of repetitive input from the armed forces. It must be centrally worked upon at a higher level. The inculcation of AI into Air Force, Army and the Navy must be budgeted. India's armed forces have a demonstrated history of lag in modernisation due to budget constraints. Unless some investment is done, the start-ups that are the vehicles for building AI will fade. Additionally, our procedures "must be amended and boosted to cater to a faster time loop for procurement and induction".¹³ Alongwith incorporating AI into defensive and offensive military equipment, cyber warfare software applications and algorithms should also be developed and put into use by the armed forces and Indian intelligence agencies. In the preceding section of the article, we saw the kind of funding DARPA received by the Pentagon in order to develop an AI app to analyse emotions and get a grasp of how the adversary's future acts might be like. The whole idea of getting to know enemy's intent is central to winning a war nowadays. Earlier wars were won by getting boots on enemy land. Today, the same could be done just by installing a piece of software on an enemy's phone or IT device.

Therefore, if AI is embedded into armed weapons (aerial/marine or land based) like UAVs with the ability to do successful facial recognition (FR) of adversary troops, it would open a whole range of new warfare possibilities

13. Lt Gen PR Shankar (Retd), "Garnering artificial intelligence for Indian armed forces", *The Daily Guardian*, June 25, 2020.

with less loss of life. How would a UAV do all this without human control/command? Take for an instance, a battalion is deployed in Leh. A few hours before dawn, there is a suspected movement detected in the valley. The UAVs get airborne for reconnaissance of the area. The InfraRed (IR) sensor, similar to those in Kalashnikov's AI guns, detect signals and quickly recognises them using the fed information. If the software doesn't see any arms/ammunition or they are not dressed in enemy uniform (as fed earlier into the software), then it does not fire. It may ask for authorisation before proceeding in this case as there is currently a popular consensus that giving robots the authority to open fire and kill humans would trample over a dangerous red line that should never be crossed. It should be taken into note that robots already exist in strenuous fields such as mine clearance, bomb disposal and anti-missile systems. As of 2021, the software is still not completely accurate to take full decisions without human interference when it comes to human life. Even today, it is advisable to have a human authorise an AI's decision.

When it comes to the aspect of AI for soft power, we must acknowledge the fact that most of the threats in cyber world or real world come through information. Most of the technologies are now publicly available to everyone. But, the one who can realise its true potential and put the tools to clever use, is the one who is going to win. It is very much possible that "India becomes the next artificial intelligence superpower through zealous innovation and consistent research and development in the technology front. The government must make sure that Indian companies and AI-entrepreneurs start investing more on research and creating India-origin AI systems and solutions. India is already known as an IT powerhouse, creating an environment conducive to the growth of AI to flourish here".¹⁴ Intelligence leaders are working to stay ahead of global AI powers like China, Israel, USA, Iraq and North Korea and to change the way they make decisions based on data. "The absolute quantity of available information would be impossible for humans to process without technological assistance of data analysis tools and AI assisted systems.

14. Anushruti Singh, "India-The next emerging superpower in artificial intelligence", SMEfutures, November 2, 2020, at <https://smefutures.com/india-the-next-emerging-superpower-in-artificial-intelligence/>. Accessed on May 30, 2021.

AI-powered surveillance can detect abnormal behaviour and mal-intent within a matter of seconds. If the same technology is installed at main gates or guardrooms of cantonments/airbases, it would not only make the establishment more secure but it could also scan intent and behaviour of every labour/civilian that enters the base, as the nervousness remains at a high point at areas such as the main guard room.

To keep up with military and intelligence agencies 'insatiable' appetite for credible information, we have to make machines integrated into all our processes".¹⁵

India must operationalise, the use of systems such as surveillance systems that include video analytics that analyse video footage in real-time and learn human intent and emotions through smart facial/emotion recognition capabilities. The use of these kinds of systems in cantonments and areas with high value assets can be enormously beneficial for security, as AI-powered surveillance can detect abnormal behaviour and mal-intent within a matter of seconds. If the same technology is installed at main

gates or guardrooms of cantonments/airbases, it would not only make the establishment more secure but it could also scan intent and behaviour of every labour/civilian that enters the base, as the nervousness remains at a high point at areas such as the main guard room. A security software with the aid of video analytics technology backed by AI learns what is ordinary so it can identify the extraordinary and harmful behaviour that a human alone tends to slip. It can do this in two ways: first by carefully witnessing objects in a perfectly monitored environment and detecting when humans and vehicles are present. Another method could be by taking operator feedback thus refining its functionality.

Thus a teachable system is created by the very interactions between the operator and his system. Artificial Intelligence functions at its best or excels in the realm of security, where eventually, human oversight takes a backseat

15. Jack Corrigan, "In a world where everyone can collect data on everything, speedy analysis could make or break U.S. national security, a top intelligence official says", NextGov.com, June 27, 2019.

to the fine-tuned competences of intelligent video analytics".¹⁶ A key driver for bringing Artificial Intelligence to security is eliminating human error.

PART 3 – SCOPE OF AI

The last decade saw the advent of means for collection and analysis of big data that goes into the decision-making. With the sophisticated computer systems, applications and cloud computing, which helps to store vast amounts of data, assists in the R&D process of deep learning, Machine Learning and AI.

We have already discussed the way artificial intelligence programme will predict a person's behaviour but we need to cite a major contributor in development of such technology which runs on a compilations of hundreds of different streams of study, be it psychology, mathematics, biology, etc. Game theory is a field of study in applied mathematics and a significant theoretical framework employed for conceiving social situations among competing players. Game theory is the science of strategy, or at least the optimal decision-making of independent and competing actors in a strategic setting. Game theory delivers a powerful framework for the design and analysis of multi-agent systems that can comprise strategic interactions. The behavioural game theory literature has industrialised a wide range of models for predicting human behaviour in strategic settings by incorporating cognitive biases and limitations derived from observations of play and insights from cognitive psychology. Predicting human behaviour has a huge variety of applications in today's world, ranging from autonomous robot navigation and human-robot collaboration to exploring atypical situations

Predicting human behaviour has a huge variety of applications in today's world, ranging from autonomous robot navigation and human-robot collaboration to exploring atypical situations in surveillance imagery and activity-aware service algorithms for a variety of purposes.

16. Dr. Mahesh Saptharishi, Avigilon, "The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology", Wired, at <https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/>. Accessed on June 1, 2021.

in surveillance imagery and activity-aware service algorithms for a variety of purposes. Consider an agent monitoring a patient's actions, activities in autonomous healthcare services, trying to predict if the patient is losing his/her balance. If it is capable of predicting the next activity, it can identify whether she or he might fall and take an action to prevent it.¹⁷

When the computer-based Artificial Intelligence systems uses a much quicker technique for learning new objects and behaviours, it can come closer to functioning like a human brain. We can imagine that if a program or a system has the skill to understand its environment and is socially intelligent, the bandwidth of possible uses in conflict would expand greatly. If a hidden application is sent to a person's phone for spying purposes, its functioning like a human brain can be as good as positioning an in-field spy.

"Humans are able to rapidly and precisely learn new visual concepts from sparse data, sometimes from just a single example. Even a four to five-month-old baby can easily learn to identify zebras and distinguish them from cats, dogs, and giraffes. But computers need to see many examples of the same object to know what it is. The computational ability of the brain rests in the potential to simplify the process of learning by leveraging formerly learned representations".¹⁸

"In 2020, The United States Air Force successfully flew an AI co-pilot on a U-2 spy aircraft in California in 2020, marking the first time AI has taken control of a U.S. military system. The computerized U-2 co-pilot, affectionately named Artup",¹⁹ took scenes from the movie Star Wars a few parsecs nearer to an aircraft near us.

Gartner, a popular research firm predicts that by the year 2022, around 10 per cent of personal devices will be fully equipped with emotion AI capabilities, allowing for a more accurate assessment of our emotional

17. Adam Hayes, "Game theory", Investopedia, <https://www.investopedia.com/terms/g/gametheory.asp>, April 28, 2021. Accessed on May 26, 2021.

18. Georgetown University Medical Center. "Tweaking AI software to function like a human brain improves computer's learning ability." ScienceDaily. ScienceDaily, January 12, 2021, at www.sciencedaily.com/releases/2021/01/210112085359.htm. Accessed on May 30, 2021.

19. Dr. Will Roper, "Exclusive: AI Just Controlled a Military Plane for the First Time Ever", Popular Mechanics, December 16, 2020, at <https://www.popularmechanics.com/military/aviation/a34978872/artificial-intelligence-controls-u2-spy-plane-air-force-exclusive/>. Accessed on May 30, 2021.

state. Prototypes and commercial products already exist around the world and are adding emotional context by analysing data points from people's facial expressions, behavioural patterns and voice intonation which will significantly enhance "the user experience".²⁰ Today our electronic devices, smartphones and wearable devices collect, analyse, and process emotional data through various sensors which are used to respond to most of the user's needs. This is already being used in the smart watches or fitness bands. Bodily functions such as heart rate, blood oxygen saturation levels, stress levels, heart rate, SpO2, etc., are recorded 24x7 on such devices.

Artificial Intelligence is also enabling realistic photo, audio, and video forgeries, also called 'deep fakes'. Adversaries could deploy these as part of their information operations to create false news reports, erode public trust, influence public discourse, and attempt to blackmail diplomats. Although most deep fakes have been found to be detectable by experts, the sophistication of the technology is advancing and it may soon be capable of hoodwinking forensic analysis tools. "AI could also be used to create what is called 'digital patterns-of-life', in which an individual's digital footprint is merged and matched with purchase histories, professional resumes, credit reports and subscriptions to generate a comprehensive behavioural profile of service members, government officials, suspected intelligence officers, or private citizens".²¹ As far as the deep fake technology is concerned, the information attained could also be used for targeted *Influence Operations*.

The fact that AI will have a revolutionary impression on tomorrow's warfare is agreed upon by a number of defence strategists and military leaders. The world of technology asserts that AI will induce a "seismic shift on the field of battle" and "fundamentally transform the way war is waged".²²

20. Cheryl Kahla, Personal devices will use AI to detect our emotional state by 2022, *Thesouthafrican*, January 19, 2021, at <https://www.thesouthafrican.com/technology/personal-devices-human-emotion-artificial-intelligence/>. Accessed on June 2, 2021.

21. Laurie A. Harris, "Congressional research Service, Deep fakes and national Security", June 8, 2021., at <https://crsreports.congress.gov/product/pdf/IF/IF11333>. Accessed on June 5, 2021.

22. Congressional Research Services, "Artificial Intelligence and National Security", updated November 21, 2019, at https://www.everycrsreport.com/files/20191121_R45178_34bc0ff0f6069c4d71e2e59e4583307811b9da44.html. Accessed on June 3, 2021.