International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Design and Implementation of Bridgeless CUK Converter with an Intelligent Controller to Efficiently Power Multiple Loads

Dharani S[1], Karthick M[2], Mohana Sundaram N[3]

[1,2]Student, Kumaraguru College of Technology

Abstract

This project presents the design and implementation of a Bridgeless CUK Converter for powering multiple loads, utilizing an intelligent control system. The converter employs a novel bridgeless topology aimed at improving efficiency, reducing component count, and minimizing power losses. A hybrid control strategy comparing PID (Proportional-Integral-Derivative) and ANN (Artificial Neural Network) is developed to ensure precise voltage regulation for various loads. The PID controller provides initial stabilization, while ANN dynamically tunes parameters to optimize performance under varying load conditions. Experimental results demonstrate the system's high efficiency, fast transient response, and accurate voltage regulation, making it ideal for applications such as IoT devices, medical equipment, and renewable energy systems that demand multiple regulated outputs.

INTRODUCTION

Artificial intelligence refers to the machine simulation of human intellectual processes, particularly in computer systems. Expert systems, machine learning, speech recognition, and natural language processing are a few specific uses of artificial intelligence. AI systems typically function by absorbing vast quantities of labeled training data, examining the data for correlations and patterns, and utilising these patterns to forecast future states. In this way, an image recognition programme can learn to recognize and characterize items in photographs by going through millions of example or a Chatbot fed text examples can learn to create realistic conversations with people. Generative AI algorithms are developing quickly and can produce realistic text, graphics, music and other media.

AI has been widely applied in a variety of fields over the past few decades, and researchers continue to debate the best ways to apply AI in these fields while maintaining safety and efficacy. AI based tech have been used in a multitude of disciplines, including political decision-making and combat, at a rate never seen before in the world's recent history. Concerns concerning responsibility, transparency and compliance with international law are brought up by the ethics of AI in hybrid warfare. There are concerns that opponents may manipulate or take advantage of AI, producing unanticipated results and intensifying hostilities. Concerning AI's ability to sway public opinion through disinformation and psychological tricks, there are further ethical issues. The swift progression of AI technology demands ongoing modifications to ethical frameworks to guarantee its acceptable and efficient application in warfare.

AIM

Aim. The aim of this research paper is to critically analyse the ethical considerations of AI in context of Hybrid Warfare.

SCOPE

The scope of this research paper is as follows: - Part I: Background of Artificial Intelligence.
Part II: Ethical Principles in use of AI in Hybrid Warfare.
Part III: Current Status of AI in Hybrid Warfare across the World.
Part IV: Roadmap of use of AI in India and Ethical Implementation in Hybrid warfare.
Part V: Futuristic Outlook and Way Forward.
Part VI: Right to Privacy and National Security

PART I

BACKGROUND OF ARTIFICIAL INTELLIGENCE

Greek mythology is where intelligent robots and artificial beings first made their appearance. Furthermore, Aristotle's use of deductive reasoning and the construction of syllogisms represented a turning point in humanity's search to comprehend its own intelligence. The history of AI is less than a century old, while having deep and extensive roots. A brief summary of some of the most significant AI related events is provided here.

Basic concepts such as Asimov's Three Laws of Robotics, the first neural network mathematical model, and Hebbian learning appeared in the 1940s. The Turing Test, the first neural network computer, and substantial advancements in AI programming and problem solving tech were all made in the 1950s. AI labs were established in the1960s, and machine translation difficulties were recognised. Budget cuts in the 1970s led to a period of declining AI development dubbed as the "First AI Winter." With the creation of commercial expert systems and large-scale initiatives like Japan's Fifth Generation Computer Systems, AI saw a rebirth in the 1980s. The "Second AI Winter" was brought on by project failures and market breakdowns in the late 1980s and early 1990s. AI underwent significant development in the 2000s and 2010s, as seen by events like IBM's Watson's Jeopardy Victory, the intro of Siri and Alexa, deep learning discoveries, and development in self-driving tech.

The tenets of ethical AI are widely accepted for good reason, they are consistent with several international declarations, treaties, and conventions, as well as internationally accepted conceptions of fundamental HR. Al's ethical precepts will be examined and critiqued. This recommendation's cornerstone is the preservation of HR and dignity. When dealing with high-risk scenarios, AI models have to be able to explain not just how they arrived at certain forecasts or selected particular actions, but also their overall decision-making process. AI systems ought to function within the constraints of their design and produce reliable, consistent predictions and judgments. It should take precautions to prevent undesirable consequences (safety risks) and exploit weaknesses (security risks). Cyber dangers, such as AI tools that rely on third parties or the cloud, should be prevented from accessing systems and the data they hold. Privacy needs to be supported and safeguarded at every stage of the Al lifecycle. It is also necessary to set up adequate structures for data protection. All systems need to be accessible and auditable. To prevent inconsistencies with HR standards and risks to the welfare of the environment, processes for oversight, impact assessment, audit, and due diligence should be in place.

The accountability for the ethical ramifications of the use or misuse of AI models should be categorically

allocated to someone, or to some organisation. Transparency and Explainability (T&E) are key components of Al systems ethical implementation. Although There may be conflicts between T&E and other values like privacy, safety, and security, the level of T&E should be appropriate for the situation. Create and run your AI with no prejudice towards any persons or organisation. Member states have an obligation to make sure that Al systems do not take the place of ultimate human accountability and responsibility. Increase the amount of human oversight and intervention in the operations of your AI models to mitigate increasing degrees of ethical risk. Respect for national sovereignty and international law is required while using data. Furthermore, inclusive methods to Al governance require participation from a variety of stakeholders. Every stakeholder must abide by all applicable laws and regulations at every point of an AI system's life cycle.

The military is making significant investments in AI & there are already instances of AI being used in weapon systems or to perform military operations on the battlefield.

Three areas that present serious concerns from a humanitarian standpoint are those that the ICRC has identified areas where AI is being researched for use by armed actors in warfare including weapon systems, especially autonomous ones, in their integration & Application in information and cyber space supporting decision support systems used by the military.

When it comes to using AI for military reasons, autonomous weapon systems have drawn the most attention. For instance, there are worries that AI might be utilised to start a collision with a person or a car. Governments are being pushed by the ICRC to enact new international regulations that would limit the use of certain autonomous weapons and forbid the deployment of others, including those under AI control.

The hazards connected with using AI in decision support systems, cyber and info operations & cyberspace have received comparatively less attention; for more detail, refer to the sections below. If the world community does not adopt a human-centered perspective when it comes to the application of AI in armed conflict, then all these applications may cause harm to people.

AI has multiple uses in Hybrid Warfare.

Cyber Operations. AI improves cyber capability both offensively and defensively, facilitating quick threat identification, quick response times, and quick adaptation to changing cyber threats.

Info Operations. AI uses massive data analysis to disseminate false info, sway public opinion, and carry out psychological tricks that make it difficult to distinguish between accurate and false info.

Predictive Analytics. AI analyses a variety of data sources to forecast adversary objective, identify patterns of behavior, and evaluate threats. This allows for better informed decision-making in unpredictable and dynamic contexts.

Autonomous Systems. AI-powered autonomous systems, such as UAVs & drones, carry out operations like surveillance and reconnaissance, lowering the danger to humans and improving operational capability.

Decision Support. Artificial intelligence (AI) helps mil leaders make decisions by evaluating complex data, coming up with other plans of action.

Al must be used ethically in hybrid warfare, and this requires careful thought to avoid abuse and unintended consequences. It is imperative to establish openness, accountability, and international collaboration in order to guarantee that Al tech conform to moral principles. It's crucial to strike a balance between humanitarian ideals and national security concerns. Prioritisation must be given to safeguards against autonomous weapon systems, privacy protection for civilians, and compliance with international

law. In order to reduce the hazards connected with Al in hybrid warfare, strong frameworks that encourage responsible Al development and deployment should be established. This will encourage a global commitment to ethical principles in this dynamic environment. [2]

1. Artificial Intelligence (AI): What Is AI and How Does It Work?|Built In
2. The Role of AI in Hybrid Warfare (mgimo.ru)

PART II

ETHICAL PRINCIPLES IN USE OF AI IN HYBRID WARFARE

Around the world, countries have always wanted to create new technologies to get an advantage over their enemies. AI has become a big topic in technology lately. Everyone has been focusing on making AI better for the past two decades. But not many people are thinking about the ethical side of AI, which is where everyone is lacking.

Countries worldwide are trying to use AI in their defence systems. For example, the latest national defence and innovation strategies of countries like the USA, UK, Singapore and China talk about AI capabilities. These capabilities are already being used to make critical national infrastructures like transport, hospitals, and energy supply safer. NATO also sees AI as a key technology to stay ahead of enemies, as mentioned in its 2020 report on the future of the alliance.

AI can be used in many ways in national defence, from helping with logistics to recognising targets and training. Military planners think AI could help defeat enemies faster.

But like with anything new, AI brings some big ethical problems. These include making conflicts worse, spying on people, spreading lies, and violating people's rights. If we don't deal with these problems, using AI in defence could go against the important values of democratic societies and world peace.

This research paper aims to help solve these problems by finding ethical principles for using AI in hybrid warfare.

Responsibility and Accountability

People should use their judgment and be responsible for the development, deployment, use, and outcomes of AI systems. Humans have legal rights and obligations, while AI systems are just tools and don't have legal or moral agency.

With increased reliance on AI systems, it may become harder to tell when a system is acting independent and potentially unlawfully. Therefore, mechanisms for assigning responsibility become more important. [3]

[3]Hohfeld, Wesley Newcomb. 1913. “Some Fundamental Legal Conceptions as Applied to Judicial Reasoning” The Yale Law Journal, No. 1: 16-59

Responsibility can be seen as a Nested Set:

1. The first layer lies with those individuals who have authority over the design, development, testing, and training for any AI system.
2. In armed conflict, a second layer concerns mechanisms for actions taken by decision-makers. This requires a robust Command and Control system.
3. The third layer involves mechanisms for actions after hostilities have ended, including holding

individuals accountable for any alleged violations.[4]

State responsibility arises from the fact that States are the principal bearers of international obligations. Acts deemed wrongful according to international law are attributable to the State itself. Therefore, any internationally wrongful acts by an organ of the State, such as the army, are attributed to the State.

Proportionality and Do No Harm

AI technologies don't automatically ensure human, environment, or ecosystem well- being. Therefore, the processes related to the AI system lifecycle shouldn't exceed what's necessary to achieve legitimate aims or objectives and should be appropriate to the context. [5]

In cases where harm is possible to human beings, human rights, communities, society, or the environment, procedures for risk assessment and measures to prevent such harm should be implemented.

The choice to use AI systems and which AI method to use should be justified by ensuring that:

1. The AI method chosen is appropriate and proportional to achieve a given legitimate aim.
2. The AI method chosen doesn't violate or abuse human rights.
3. The AI method is appropriate to the context and based on rigorous scientific foundations.

In scenarios involving irreversible or life-and-death decisions, final human determination should prevail. AI systems shouldn't be used for social scoring or mass surveillance purposes.

[4]Department of Defense Dictionary of Military and Associated Terms. July 2019.

[5]UNESCO ethical recommendations https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

Right to Privacy and Data Protection

Privacy is essential for protecting human dignity, autonomy, and agency. Throughout the AI system lifecycle, data should be handled in ways consistent with international law and relevant legal frameworks. Adequate data protection frameworks and governance mechanisms should be established, ensuring a legitimate aim and a valid legal basis for the processing of personal data, including informed consent.

Algorithmic systems require privacy impact assessments, including societal and ethical considerations, to maintain privacy throughout their lifecycle.

Traceable

AI engineering discipline should provide technical experts with an understanding of AI systems, including transparent and auditable methodologies, data sources, and design procedures and documentation.

Ensuring AI traceability involves providing relevant stakeholders with information during development and deployment phases.[6]

Reliable

AI systems should have an explicit, well-defined domain of use, and the safety, security, and robustness of such systems should be tested and assured across their entire life cycle within that domain of use.

We should have a long-established history of test and evaluation (T&E) and verification and validation (V&V) of its AI systems. In high-risk areas, such as with nuclear weapons, there also exists additional programme for authority, safety, and reliability (i.e. nuclear surety). As AI will be employed across a wide

variety of apps – from enterprise systems to weapon systems – it is crucial that individual AI systems and interacting AI systems are assured appropriately.

While AI systems that we intend to use for less risky purposes may not have the same level of rigorous testing, all AI systems need to be reliable with respect to their safety, security, and robustness continually and across their life cycles and domains of use. We can think, then, of reliable AI systems as those which appropriately, safely, and robustly act within their domain.

Explainability of ML models may also be another route toward verification. There may be a need for explainable AI – the ability of an AI solution to explain the logic behind a recommendation or action.

[6] We use "traceable" as the overarching principle here to align with the "Organisation for Economic Cooperation and Development's Principles on AI", which the U.S. approved, along with 42 other countries, in May 2019.

Explainability refers to making intelligible and providing insight into the outcome of AI systems. The explainability of AI systems also refers to the understandability of the input, output and the functioning of each algorithmic building block and how it contributes to the outcome of the systems. Thus, explainability is closely related to transparency, as outcomes and sub-processes leading to outcomes should aim to be understandable and traceable, appropriate to the context. AI systems should commit to ensuring that the algorithms developed are explainable. In the case of AI applications that impact the end user in a way that is not temporary, easily reversible or otherwise low risk, it should be ensured that the meaningful explanation is provided with any decision that resulted in the action taken in order for the outcome to be considered transparent.

The level of explainability or assurance should depend on the nature of the mission, with higher assurance required for scenarios involving risks.[7]

[7] ArtificialIntelligence–AkeyenablerofhybridwarfarepaperbyRalphThiele http://www.hybridcoe.fi/for enhancing EU-NATO hybrid warfare technologies.

PART III
CURRENT STATUS OF ARTIFICIAL INTELLIGENCE IN HYBRID WARFARE ACROSS THE WORLD

Why are countries shifting to Hybrid Warfare. Conventional Warfare poses direct threat on economy of the countries, inflicting huge casualty on both sides and increased fear of sanctions from the global forum.

Hybrid Warfare involves using non-conventional techniques and indirect warfare to destabilize the rivals and gain tactical advantage.

"Hybrid Warfare aids a country to gain Tactical Advantage against other nations"

Incorporating AI to fight Hybrid Warfare increases the capability and efficiency of the attack and gives the desired result in short timeframe. In the recent times, many countries have used AI in Hybrid Warfare to achieve varied results and were successful in achieving the same. Some of the examples of the technologies used and ethical challenges while using those technologies are mentioned as follows.

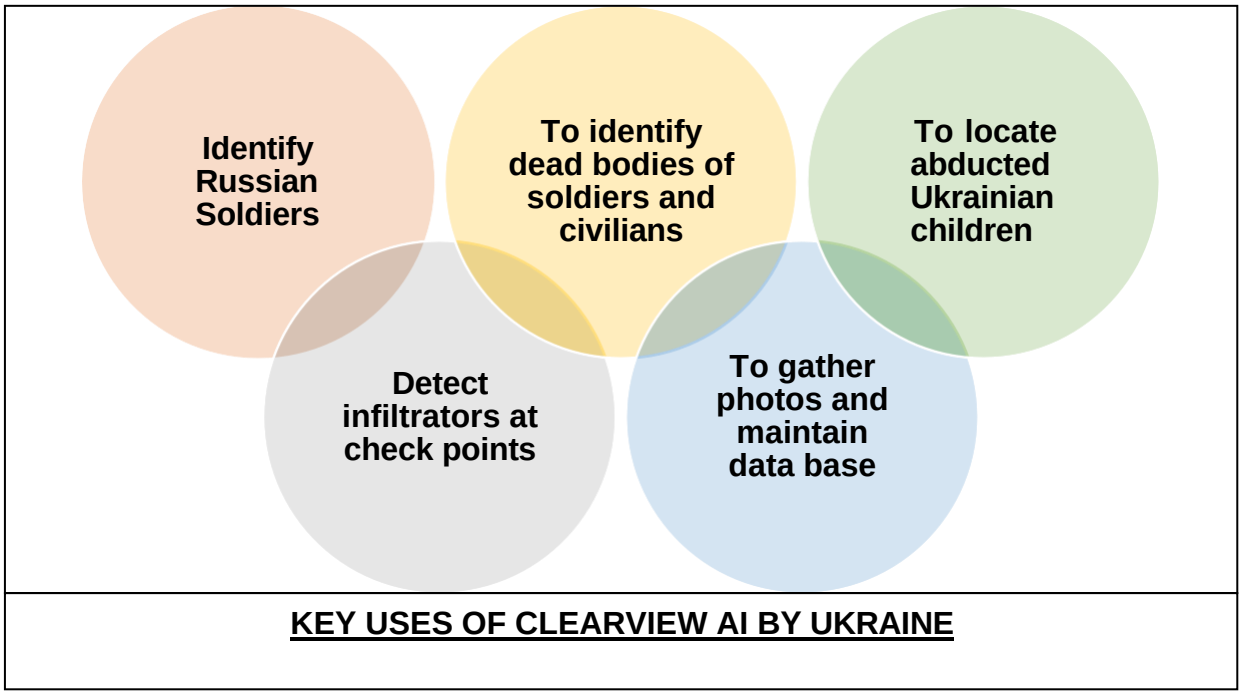
Use of AI by Ukraine against Russia

In the war against Russia, Ukraine has used the software, made by the American facial-recognition

company called '**Clearview AI**'. Clearview AI is termed as Ukrainians' Government "Secret Weapon".
About Clearview AI. Clearview AI is a facial recognition tool developed by U.S. startup. After the war between Ukraine and Russia broke, Clearview foundation has offered their assistance to Ukraine's Government to detect Russian soldiers, missing Ukrainian civilians and to stop false propaganda[8]. Clearview maintained a database of human faces collected all across the social media and internet. When the Ukrainian Government tested this application against the intruded Russians, it gave 99.85% accuracy. Ukrainian officials have used Clearview to detect infiltrators at checkpoints, process citizens who lost their IDs, identify and prosecute members of pro-Russia militias and Ukrainian collaborators, and even to locate more than 190 abducted Ukrainian children who were transported across the border to live with Russian families. More than 1,500 officials across 18 Ukrainian Government agencies are using the facial-recognition tool, which has helped them identify more than 2,30,000 Russian soldiers and officials who have participated in the mil invasion.

[8]**https://www.clearview.ai/ukraine**

Key uses of Clearview AI by Ukrainian Government against Russia.



Ukrainian Government also used Clearview AI to counter the propaganda spread by Russian News Channels and it also opened a website where the detail of Russian soldiers who infiltrated into Ukraine territory are updated. Many families of Russian soldiers used this website to check the status of the soldier "whether he is alive or not". This had huge psychological implications and the Russian soldiers were forced to use face mask in hot humid conditions to avoid being detected by the Clearview technology.
Use of Turkish TB2 Bayratkar. "Turkish TB2 Bayraktar" a remotely piloted killer drone with a range of up to 190 miles manufactured by Turkish company. The TB2's ability to carry multiple air-to-ground munitions helped Ukrainian forces to penetrate Russian air defences and strike heavy targets. However, as time pronged and Russia took greater control of the skies, it was able to detect and shoot down these larger models of TB2 more easily.
Ukraine has shifted the role of TB2 from offensive role to reconnaissance and controlling arty fire and

assisting other small drones. Ukraine has focused on development more sophisticated TB3 drones with help of Turkey. Around 30 countries across the world are using TB2 drones for various purposes.

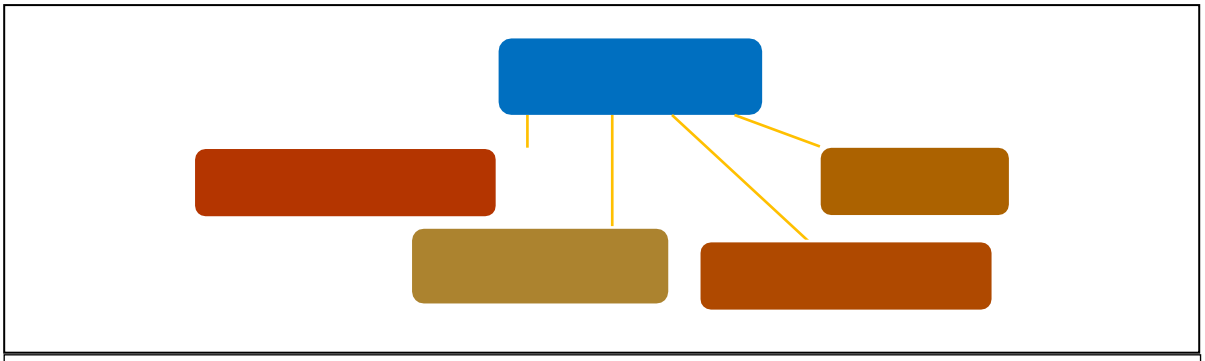
Challenges

A. The "Clearview" AI technology used for face recognition raises inaccurate data concerns as misidentification could lead to severe problems like mistaking civilians for soldiers.
B. Gathering photos and maintaining in database, accessing social media accounts and internet sites without owner's consent raises ethical and privacy concerns and the sensitive data can be misused.
C. The use of autonomous weapons like TB2 powered by AI could raise concerns about the lack of human control over decision-making in conflict situations. This could lead to unintended consequences, escalation, and a higher risk of civilian casualty.

Use of Artificial Intelligence by Israel

Israel has determined to become a power house in the field of Artificial Intelligence to boost their capability in autonomous warfare and to make smarter decisions in combat.

USES



USES OF AI BY ISRAEL

classification of Hamas Terrorists

Fire Factory: AI for Logistics. Israel has incorporated AI into mil operations to improve logistical calculation and speedup the decision-making processes. When a target is given to "FireFactory", the application calculates the data regarding the ammunition and logistics required, allocates the target to fighter jets and mil drones and also generates a schedule. This minimises the time required to take for calculation of the same and more importantly it rules out human error. Though the entire data is calculated by AI, still the final decision of executing is with human.

Iron Dome. Iron Dome, a defence sys that uses radar technology, was primarily designed to intercept short-range rockets and mortars targeted at Israel. Its op involves the utilisation of predictive analytics and machine learning to identify and neutralise incoming projectiles. The sys can detect an incoming rocket from distances of up to70 kilometers by considering various factors such as speed, weather conditions, and the projectile's size to accurately calculate its trajectory and potential point of impact. Upon gathering this critical data, the control centre carefully analyses it and, when necessary, deploys a counter-missile to intercept and eliminate the en rocket threat. If the system determines that a rocket is headed towards an unpopulated area where there will be little or no damage, it may opt not to engage.[9]

Assassination of Iran's Nuclear Scientists. When Iran Government had decided to work on its nuclear program, Israel had carried out multiple assassinations of Iranian nuclear scientists in Iran. Iran had accused Israel's involvement in these assassinations whereas the Israel Government has neither accepted nor denied the same. This is one of the best examples of Hybrid Warfare where one country showed dominance over the other without getting conventionally involved.

In the sequence of these assassinations, Israel had used AI powered robot to kill the Iranian top scientist Mohsen Fakhrizadeh – Father of Iran's nuclear program. In this mysterious event, a truck was equipped with a computerised FN MAG Machine Gun attached to an advanced robot powered with Artificial Intelligence and explosive. The AI was programmed to compensate for the delay, the shake, and the car's speed and as soon as the AI detected the target, it had fired 13 rounds neutralised 'Mohsen Fakhrizadeh'. As soon as the target was neutralised the truck blew itself leaving no traces behind. The system was so accurate that not even a single bullet hit neither his wife who was sitting beside him nor any of his bodyguards. An assassination done directly might have escalated into war, this left everyone mysterious regarding the operator and whom to blame.[10]

[9]**https://www.firstpost.com/tech/news-analysis/modern-warfare-how-israel-is-neutralising-and-pushing-out-hamas-using-ai-13227072.html**

[10]**https://www.timesofisrael.com/mossad-killed-irans-top-nuke-scientist-with-remote-operated-machine-gun-nyt/**

Challenges

a. 'Fire Factory'- helps in saving time and taking a timely and accurate decision in adverse situation. It also has the potentiality of resource allocation wherein based on the data given, it can allocate the target to a specific jet or a resource. As long as the human is intervening these decisions and taking the final call, the damages can be controlled. But when this system becomes autonomous, a single wrong decision can lead to heavy casualty.
b. The assassination of Iran's nuclear head 'Mohsen Fakhrizadeh' using a remotely op vehicle powered by AI was a eye opener to the entire world. Use of such AI assisted systems in future for carrying out special tasks will increase accuracy and reliability. But when these technologies land in the hands of terrorist groups, it becomes a grave concern for the state to deal against the same.
c. Use of AI by China

Data Collection using AI. The Chinese company "Zhenhua Data Information Technology" is alleged against monitoring data of key persons and organisations across the world. Zhenhua uses Artificial Intelligence to monitor digital footprint across social media platforms, papers, documents and open source. Though the Chinese Government denied any connections with this company, this info can be used for strategic and intelligence services of China for Hybrid Warfare.

The Great Firewall. The Chinese Government's "Great Firewall" is a well-known example of how AI-based algorithms are employed to monitor and control public opinion within the country. The system consists of a combination of machine learning algorithms and human moderators to filter incoming info from the World Wide Web, blocking foreign propaganda and politically sensitive content from reaching Chinese citizens. The Great Firewall works by using AI to monitor Internet traffic and social media

platforms for keywords and topics that are considered politically sensitive by the Government filters and blocks content containing them. The sys allows the Government to effectively control what info is available to Chinese citizens.[11]

Challenges.

a. 'Great Firewall'- is one of the classical example of driving the nation towards singular objective. By restricting the content to internet users, China is violating 'Right to Information' and objecting their free decision taking capability. These AI based applications can be used for Narrative building and to Counter Propaganda in Info Warfare domain.
b. The data collected by Zhenhua Company is still not validated and authenticated and violates Right to Privacy. This data can be used by State and Non State actors for malicious activities and the affected database will not even be aware of the damage caused to them.

[11]**https://sgpjournal.mgimo.ru/2022/2022-10/ai-role-in-hybrid-warfare**

Analysis

The world has shifted from Conventional Warfare to Hybrid Warfare and using Artificial Intelligence, the capability of the sys are going to increase multifold.

Rank	Country	2023 investments (millions USD)	% of investment increase compared to 2019	Total investment in last 5 years (millions USD)
1	United States	67,911	65.9%	328,548
2	China	15,071	-30.5%	132,665
3	United Kingdom	3,518	0.2%	25,541
4	India	3,808	261.3%	16,147
5	Germany	1,808	-11.2%	14,300
6	Canada	2,067	40.2%	12,457
7	South Korea	2,102	238.5%	10,348
8	France	1,853	74.7%	10,185
9	Sweden	2,603	2310.2%	8,281
10	Singapore	1,928	191.7%	7,005

(Source: AIPRM via OECD and World Bank) techeconomy

INVESTMENT IN AI BY VARIOUS COUNTRIES

In terms of investments in AI, US continued to remain at top followed by China whereas India has showed

a significant increase in investment of 261% compared to 2019. In 2022, the Government of India published a list of 75 priority projects related to using AI for defence; these projects focused on data processing and analysis, cyber security, simulation and autonomous systems, particularly drones. India is also exporting AI applications for underwater domain awareness and border security.[12]

[12]Use of AI in defence. https://www.liss.org/

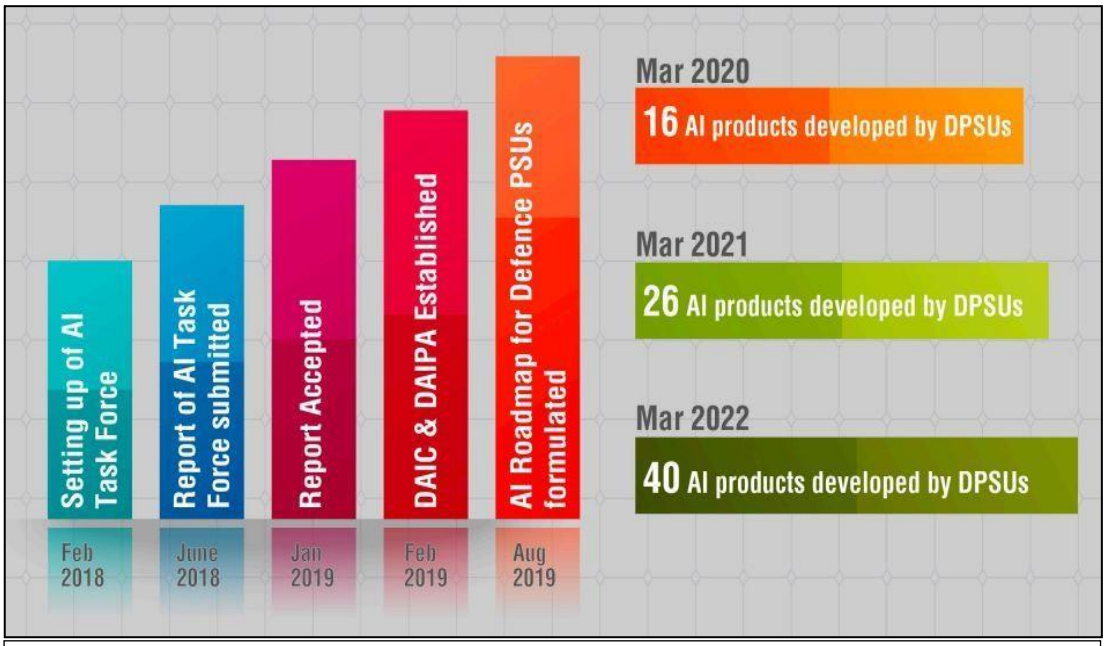
PART IV
ROADMAP OF USE OF AI IN INDIA AND ETHICAL IMPLEMENTATION IN HYBRID WARFARE

In this part we look at the current status of employment of AI by Defence forces of India and delve into systems and technologies currently using AI for hybrid warfare in Indian Armed forces. We will also go through ethical considerations of these systems using AI for warfare and how can we have a responsible framework to create future ready systems.

Roadmap of implementation of AI in Armed Forces.

Artificial Intelligence is shaping India's defence landscape providing the army with augmented capability for functioning in diverse domains of hybrid warfare. The Indian defence industry is taking giant steps in transforming the armed forces into one of the most advanced in the world. The adoption of technology based on Artificial Intelligence (AI) will revolutionise the Indian Military in fighting the modern multidomain hybrid warfare. It also places India firmly in the huge defence product market. Along with enhancing its operational capabilities, the Indian Defence forces have been deploying Artificial Intelligence and surveillance systems along its borders with China and Pakistan, thus enhancing its operational efficiency and preparedness. This joint effort among industry both public and private, research organisations, academic institutions, start-ups and innovators have helped create many unique technological products based on AI in the areas of data, logistics, surveillance, weapons and many more. The Government has taken significant steps to ensure integration of AI into Armed Forces.

On 25 Aug 2017, the Ministry of Commerce and Industry constituted the “Task Force on AI for India’s Economic Transformation”. The 18 member Task Force, chaired by Professor V Kamakoti of IIT Madras, consisted of experts from academia, research laboratories and industry. In addition, the Taskforce also had Government officials from the Ministry of Commerce and Industry, Ministry of Electronics and Information Technology, Ministry of External Affairs and DRDO. The Task Force submitted its report on 19 January 2018. It suggested the creation of a National AI Mission as a nodal agency for coordinating AI related activities in India, with a budgetary allocation of 1200 crores over five years.



ROADMAP OF IMPLEMENTATION OF AI IN INDIA BY DEFENCE FORCES

(Source: Dept of def prod, Government of India)

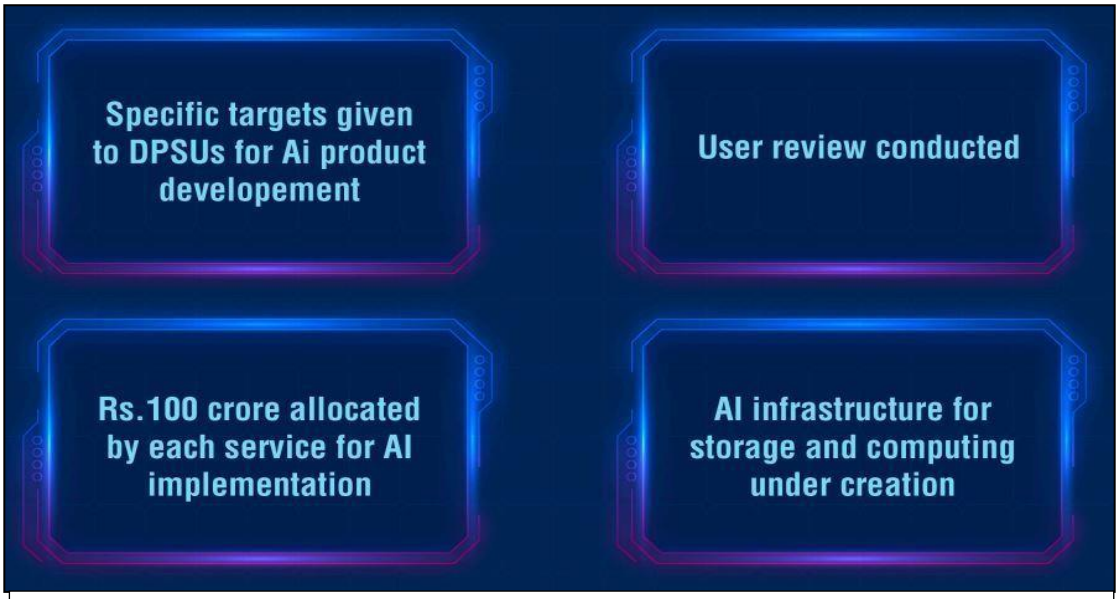
On 02 February 2018, the Department of Defence Production (of the Ministry of Defence) constituted a Task Force to study the future use of AI in defence applications. Known as the Task Force for 'Strategic Implementation of AI for National Security and Defence', it was headed by Tata Sons Chairman N Chandrasekaran. The other 16 members in the Task Force included National Cyber Security Coordinator Gulshan Rai, Chairman & Managing Director of Bharat Electronics Ltd., and representatives from the Army, Navy, Air Force, Indian Space Research Organisation, Atomic Energy Commission, Indian Institute of Science (Bangalore), IIT (Bombay), IIT (Madras) and private industry.

For Military use, the Functional Areas were Lethal Autonomous Weapon Systems (LAWS), Unmanned Surveillance, and Simulated War Game & Training. For dual use, the Functional areas were Cyber security, Aerospace Security, and Intelligence & Reconnaissance. The Task Force submitted its report to the Raksha Mantri (RM) on 30 June 2018

Defence forces of India have deployed about 140 AI-based surveillance systems, which include high-resolution cameras, sensors, unmanned aerial vehicle (UAV) feed and radar feed. These are then collected and applied through AI based systems, all in the name of detecting intrusions at borders while classifying targets thus providing potential advantage in operations while also enhancing border security. AI-based real-time monitoring software has also been deployed for generating intelligence in counter insurgency and counter terrorist operations across various disturbed locations in the country.

The army has also begun leveraging hi-tech military simulator technologies to train its first batch of recruits, a trend that is likely to mark its prevalence across military training in the near future.

AI can be a game-changer in logistics, information operations, intelligence collection and analysis. Though India's adoption of military AI technology is relatively recent, we have made substantial progress in launching AI- *enabled military devices.*[13]



PROJECT TIMELINE FOR DPSUs

(Source: Dept of def prod, Government of India)

Existing and planned projects in Armed forces with Ethical Issues on their use.

The armed forces have been exhaustively brain storming and simultaneously implementing AI in its everyday functioning across various domains. As per the list compiled by Ministry of Defence, the broad division has been outlined along with niche technologies in each of it. With the evolving warfare capabilities of nations across the globe it is imperative that we as a nation are prepared to deal with multi domain and hybrid warfare. Below is a list of technologies and equipment incorporating AI.

AI in Platform Automation.

Deepcatch Edge AI Platform
Merlin ML Operations
iSentinal

[13]**https://www.ddpmod.gov.in**

System for Disseminated parallel control for competing

Autonomous/Unmanned Robotic Systems.

Sapper scout–Mine detection GV
AI capability in swarm drones
Projection drone feed analysis
Silent sentry (Rail mounted robot)
Autonomous fast intercept boat
Project storm drone
Cognitive radar
AI enabled remotely operated vehicle
HR Chatbot - Anvesha

AI powered unmanned ground vehicle

Block Chain based Automation.
Permissive block chain mechanism
AI-Based Intercept Management System (IMS)

C4ISR Systems.
AI based motion detection system
Continuously Observing Ubiquitously Available surveillance system
AI-Enabled Airborne Electro-Optic Infrared System
Deep Learning Toolkit for Aerospace and Defence
Adversary Network Analysis Tool (ANANT)
Target Tracking for Complex Naval Scenarios
Animal Detection for Railways
Enemy aircraft activity recognition and classification
AI-Based Anomaly Detection for Maritime Domain
Passive ranging using AI as a classifier
AI-Based Passive TWS (Track While Scan) System
Development of Machine Algorithms for Maritime anomalies
Enhancing UDA by use of AI/ML and other Novel Techniques
AI/Big Data for Acoustic and Magnetic Signature Analysis

Cyber Security.
Android Malware Detection Solution

Human Behavioral analysis.
Driver Fatigue Monitoring system

Intelligence Monitoring Systems.
Project Seeker – Facial Recognition System
V-logger Vehicle Tracking System
Face Recognition System under Disguise
Segmentation of satellite panchromatic videos
AI based view monitoring camera
HUMS ground station
AI based satellite image analysis
AI based prediction of atmospheric visibility
Chimera 22 Smart camera
Deep sight canopy inspection for fighter jets

IoBT.
Internet of Battle Things (IoBT): Smart Helmets
Automatic Number Plate Recognition for Smart Cities

AI enabled adaptive traffic optimisation solution

Lethal Autonomous Weapon System.
Smart countermeasures dispensing system
Adaptive front towing gun vehicles for Artillery[14]

Artificial intelligence is often thought of as the process of creating intelligent behavior using software rather than human methods. It is a form of automation and it raises some of the same issues as other forms of automation, but also some new ones because it focuses on data rather than machines. Most ethical theories place the blame for unethical behavior of algorithms on their creators and the data on which the model has been trained. It is also imp to note that the data collected and collated can be biased and the time it was digitised or created has to be taken into consideration. Some of the ethical issues that can be envisaged in usage of current AI systems used by or nation are as stated

(a) The potential for AI systems to violate international and national laws and rules of engagement, leading to disproportionate or indiscriminate attacks.
(b) Possibility of AI systems to be biased or discriminatory in their decision- making, as they are trained on datasets that may reflect existing biases and prejudices.
(c) The need to ensure transparency and explainbility in AI systems used in hybrid warfare, so that the decision-making processes can be understood and scrutinised.

[14]**https://www.ddpmod.gov.in**

The ethical implications of understanding the political decision-making of AI systems in hybrid warfare, as this raise concerns about human dignity and responsibility.

(d) The potential for AI to be used in propaganda and disinformation campaigns, leading to the manipulation of public opinion and undermining democratic processes of or nation.
(e) Potential for AI systems to be hacked or manipulated, leading to unintended consequences and potentially escalating conflicts.
(f) Potential for AI systems to create a power imbalance in hybrid warfare, where nations with advanced AI capabilities have an advantage over those without such capabilities. It is an example of proxy war in terms of AI.
(g) The need to maintain protection of civilian populations as priority and minimise harm during hybrid warfare operations, as AI-powered systems have the potential to cause collateral damage or indiscriminate killing without understanding its consequences.
(j) Innately target non-combatants and people not involved directly in a conflict or war.
(k) The importance of considering the broader societal impacts and involving stakeholders in the development and deployment of AI systems used in hybrid warfare.
(l) Training of the algorithm need to be monitored as this is the baseline for all decisions made subsequently by the algorithm and systems where the algorithm is deployed.

Methods to mitigate Ethical Concerns for use of AI in Hybrid Warfare

To enhance the use of AI in hybrid warfare encompassing the ethical backdrop, strict adherence to international laws and ethical guidelines is crucial. Implementing transparent decision-making processes,

promoting human oversight, and fostering global collaboration for ethical AI development are key steps. Regular checks and assessments by internal and external teams can ensure AI systems align with ethical standards, minimising potential risks and ensuring responsible use in military applications. Some of the suggested ways in which our nation can progress towards implementing ethical standards in AI and its related technologies are as below

Adherence to International and National Laws. It is imperative to establish a robust framework that aligns AI applications in warfare with international and national laws such as the Geneva Conventions and Indian war strategy. It is also necessary to ensure compliance with ethical guidelines, emphasising respect for human rights and minimising harm to civilians.

Transparent Decision-Making. We need to design AI systems with transparent decision-making processes to understand how conclusions are reached and what methods and codes are employed to reach that. The developer must be able to provide clear explanations for AI-generated recommendations, enhancing accountability and trust.

Human Oversight. Incorporating a significant level of human oversight and interference in AI-powered military systems to maintain accountability and responsibility of decisions made on the battlefield. Humans should retain control over critical decisions, preventing fully autonomous actions that may lead to unintended consequences.

Global Collaboration. It is necessary to foster international collaboration among nations, researchers, and organisations and academia to establish shared ethical standards for AI in warfare. We can also focus on creating a rule book for the same. Collaborative efforts can lead to better practices, reducing the risk of unethical use and ensuring a collective commitment to responsible AI.

Regular Audits and Assessments. It is very necessary to conduct routine audits and assessments both internal and external to monitor AI systems used in warfare to identify potential ethical concerns. Regular reviews can help address biases, rectify issues, and ensure ongoing compliance with ethical standards. The systems can also be tested in mock simulations for test their battle worthiness.

Ethical Training and Education. We need to provide ethical training to military personnel involved in AI-related decision-making and equipment handling. Awareness of stakeholders on the ethical implementation of AI, fostering a culture of responsible use within military organisations is absolutely necessary before deploying these systems.

Humanitarian Considerations. Humanitarian considerations must be the priority when such systems are deployed in conflict zones. We also have to ensure that AI applications are designed to minimise harm to civilians and adhere to principles of proportionality and distinction between combatants and non-combatants.

Public Accountability. Our constant endeavor must be to enhance public awareness and involvement in discussions about AI in warfare. Fostering transparency and accountability by keeping the public informed about the development, deployment, and ethical considerations of AI systems in military contexts is an important facet in today's multispectral connected world.

Bias Mitigation. Implement measures to identify and mitigate biases in AI algorithms used in military applications. Regularly assess and address any discriminatory outcomes to ensure fairness and equity. The biases in the datasets being sets used for training also need to be considered while training the module.

Redundancy and Fail-Safe Mechanisms. It is necessary to develop redundancy and fail-safe mechanisms to prevent unintended consequences in AI decision-making due to failure of systems and technical glitches. We can establish protocols for human intervention in case of system malfunctions or

unforeseen ethical challenges.

Ethical Use of Lethal Force. It is necessary to define strict guidelines for the ethical use of lethal force by AI systems from its programming stage itself. Clear articulation of the circumstances under which AI-powered weapons are authorised to engage and well defined rules of engagement, minimising the risk of misuse.

Continuous Ethical Review Boards. We have to establish independent ethical review boards to monitor and evaluate the ethical implementation of AI applications in warfare. These boards can provide ongoing assessments and recommendations for improving ethical practices.

Proactive Stakeholder Engagement. A dire need arises to engage with a diverse range of stakeholders, including ethicists, human rights organisations, and impacted communities. Proactively seeking input to address ethical concerns and incorporate diverse perspectives in AI decision-making processes will help in creation of responsible and robust systems.

Regulation and Legislation. Develop and enforce regulatory frameworks and legislation specifically addressing the ethical use of AI in military operations. Legal frameworks can provide clear guidelines and consequences for violations of ethical standards also making the developers more accountable for their programs and systems.

By integrating these measures, it's possible to cultivate an ethical framework that guides the development and use of AI in warfare, minimising risks and upholding human values. It is imperative that a watchdog organisation be formed at this early Stage to implement ethical considerations in development of AI technologies before its too late to take control of the machines back in our hands. Although this entire domain is still in development phase and many countries are still experimenting various systems, it is necessary to act before the damage is done and the algorithms overtake s to a level from where there is no coming back.

PART V
FUTURISTIC OUTLOOK AND WAY FORWARD

The ethical considerations for using AI in hybrid warfare revolve around issues like transparency, accountability, and avoiding harm to civilians. India's unique challenges and aspirations and a desire to assume leadership in this new technology means India's approach towards Al strategy has to be balanced for both mil advance and greater good. The way fwd for India in Al requires large scale transformational interventions, primarily led by the Government, with private sector providing able support.

Transparency. Promote transparency in AI systems to enhance accountability, allowing for scrutiny and understanding of decision-making processes. Transparency in the ethical considerations of AI within hybrid warfare involves openly disclosing the specific objective, decision-making and potential repercussions associated with the deployment of AI technologies in mil settings. This transparency extends to a commitment to adhering to ethical guidelines, international laws, and fundamental human rights principles throughout the entire life cycle of AI development and application in hybrid warfare. By fostering clear communication, organisations and Governments can build trust, address public concerns, and actively promote responsible practices within this complex and evolving landscape.

Legal Framework. To develop and strengthen international legal frameworks ensure compliance with human rights and ethical principles. Establish a legal framework for ethical considerations in deploying AI within hybrid warfare involves aligning practices with existing international laws like the Geneva Conventions. This ensures that AI applications adhere to human rights standard, minimising the risk of

violating laws governing armed conflicts and safeguarding civilians. Crafting explicit legal guidelines addresses the unique challenges posed by AI in hybrid warfare, emphasising accountability and compliance with ethical standards, while also potentially necessitating new legal frameworks.

Ethical AI Education. Integrate ethical AI education into mil training programme, emphasising the responsible deployment and oversight of AI technologies. Educating individuals on Ethical AI is crucial for addressing considerations in the use of AI in hybrid warfare. This involves providing comprehensive training on the responsibility development, deployment and monitoring of AI technologies within military contexts. Ethical AI education ensures that stakeholders, including developers and decision-makers, are equip with the knowledge to navigate complex ethical dilemmas and uphold principles such as transparency, accountability, and respect for human rights. This proactive approach promotes a culture of responsible AI use in hybrid warfare scenarios.

Human Loop Design. Human oversight to ensure humans remains integral in decision-making processes to prevent autonomous actions with severe ethical consequences. Integrating a human loop design into the ethical considerations of AI in hybrid warfare involves creating mechanisms for human oversight and intervention throughout the AI decision-making process. This ensures that human judgment and ethical reasoning are incorporated, allowing for intervention in situations where AI may pose ethical concerns or unforeseen consequences. The human loop design serves as a safeguard, reinforcing accountability and ethical values in the deployment of AI technologies within mil contexts.

Data Privacy and Surveillance. AI systems depend on the amounts of data like personal and professional data for decision making and targeting. Potential misuse of personal data for surveillance and profiling. Violation of privacy rights is a ethical concern. There are few recommendations for implementation of strict data protection measures, privacy rights and clear guidelines for ethical collection and use of data.

Research and Development. Encourage within ethical boundaries, fostering innovation avoids the creation of AI systems that creates ethical risks. In the research and development phase of AI for hybrid warfare, ethical considerations are paramount. This involves prioritising responsible innovation by incorporating ethical guidelines into the design, testing, and implementation processes. Researchers must be vigilant in addressing potential biases, ensuring transparency, and upholding human rights principles. Establish ethical protocols early in the R&D stage helps mitigate risks, fosters accountability, and promotes the development of AI technologies that align with ethical standards in the complex landscape of hybrid warfare.

Key Aspects. To ensure adequate privacy, security and IP related concerns and balancing ethical considerations with need for innovation. Key aspects of ethical considerations in the use of AI in hybrid warfare include transparent disclosure of objective and decision-making processes, alignment with existing international laws and human rights principles, integration of a human loop design for oversight, proactive ethical AI education, and a focus on responsible research and development. Ensuring accountability and fostering transparency are critical to navigating the ethical complexities associated with deploying AI tech in mil contexts.

One of the key aspects of our ambition includes responsibility AI ensuring adequate privacy, security and IP related concerns and balancing ethical considerations with need for innovation. Our final set of recommendations lay down the challenges and suggestion for addressing some of these not so straightforward implementation challenges of AI.

The recommendations in the following chapters are aimed at initiating an informed conversation on India's future roadmap for AI, and are descriptive rather than prescriptive by design. The paper should be

seen as providing framework for developing National Strategy for AI, and as such we have consciously avoided providing specific funding targets and funding mechanisms, as these require broad.

PART VI
RIGHT TO PRIVACY & NATIONAL SECURITY

Achieving a delicate equilibrium between the right to privacy & national security with AI involves navigating intricate considerations. Legal frameworks, transparent practices, data minimisation & international cooperation are pivotal. Striking a balancedemands ongoing efforts to ensure responsible AI use, safeguard individual rights & maintaining public trust in an evolving technological landscape. Navigating this balance requires careful consideration of various factors. Here are some key considerations:

Legal Frameworks.

The establishment of clear legal & ethical frameworks is pivotal in navigating the intricate interplay between the right to privacy & national security in the realm of Artificial Intelligence (AI). To strike a delicate balance, robust laws & regulations must be in place to delineate the permissible boundaries of AI usage, especially concerning privacy & national security concerns. These legal frameworks provide a structured & principled approach to guide Government agencies in the responsible deployment of AI technologies.

Transparency is crucial in fostering public trust. Clear, accessible & comprehensible legal frameworks demystify the intentions behind AI applications, assuring citizens that their privacy is respected & protected. Transparent frameworks enable individual to understand how their data may be utilised for national security purposes, contributing to an informed citizenry & reducing apprehensions about potential misuse.

Furthermore, the emphasis on fairness within these frameworks is crucial. The rules & regulations governing AI must be consistently applied across diverse contexts & demographic groups to prevent discriminatory practices. Fairness ensures that the benefits & risks associated with AI application are distributed equitably, reinforcing a sense of justice & inclusivity.

In essence, the establishment of legal & ethical frameworks provides a structured foundation for responsible AI deployment. Transparency & fairness are integral comps that not only bolster public trust but also underscore the commitment to upholding individual rights while addressing national security imperatives. As technology continues to advance, these frameworks must remain adaptive & responsive to emerging challenges, ensuring a resilient & ethical approach to the use of AI in the context of privacy & national security.

Data Collection & Retention.

In the intricate landscape of balancing privacy rights with national security concerns in the realm of AI, the principles surrounding data collection & retention play a pivotal role. Limiting the scope of data collection to what is strictly necessary for national security purposes is paramount in safeguarding individual privacy. Governments must ex prudence & precision, avoiding unnecessary intrusion into the private lives of citizens. Striking this balance ensures that security measures are targeted & proportionate, minimising the risk of unwarranted invasions into personal spaces.

Equally crucial is the establishment of stringent guidelines governing the retention & storage of collected data. This involves defining clear parameters for the duration & purpose of data retention, minimising the

risk of misuse & unauthorised access. Setting these guidelines helps build a framework that prioritizes the protection of individual privacy rights while allowing for the necessary storage of information crucial to national security efforts.

By implementing such measures, Governments can demo a commitment to responsible data management practices. Transparent communication regarding the specific purposes for which data is collected & the duration for which it will be retained fosters public understanding & trust. Moreover, adherence to strict guidelines mitigates the potential for abuse, ensuring that sensitive information is handled with the utmost care & in accordance with establishing ethical & legal standards. In essence, the prudent limitation & careful management of data collection & retention are foundational elements in achieving a harmonious balancebetween national security imperatives & the protection of individual privacy rights in the age of AI.

Transparency & Accountability.

Transparency & accountability are indispensable pillars in maintaining public trust & fostering responsible usage of (AI) for national security purposes. Firstly, Governments & organisations must prioritise transparency by openly communicating their methodologies, objectives & the extent of data collection associated with AI initiatives. Transparency engenders a sense of trust among the public, enabling individual to understand the rationale behind AI applications in national security & the implications for their privacy rights. By providing clarity on how data is gathered, processed, & utilised, Governments & organisations enhance accountability & encourage informed citizenry.

Moreover, establishing robust accountability mechanisms is essential to address any potential misuse or abuse of AI technologies. Accountability ensures that stakeholders are held responsible for their actions, promoting adherence to ethical standards & legal regulations. This may involve implementing oversight bodies, regulatory frameworks, or internal auditing processes to monitor the deployment of AI systems & evaluate compliance with established guidelines. In cases of misconduct or breaches of privacy, accountability mechanisms enable swift action to rectify the situation & mitigate harm.

Furthermore, accountability fosters a culture of responsibility & integrity within organisations, encouraging ethical decision-making & risk management practices. By holding individual & entities accountable for their actions, public confidence in AI applications for national security is bolstered, strengthening the legitimacy of Government initiatives in this domain. Ultimately, transparency & accountability serve as cornerstones for building & maintaining trust in the responsible use of AI technologies, ensuring that national security objectives are pursued in a manner that respects individual rights & societal values.

Minimisation of Intrusion.

The minimisation of intrusion is a critical facet in reconciling the imperative of effective national security measures with the protection of individual privacy in the context of artificial intelligence (AI). One key strategy is the adoption of advance techniques, include anonymisation & data aggregation, which serve to attenuate the level of intrusion into individual lives. Anonymisation involves the removal or mod of personally identifiable information from datasets, thereby preserving privacy while still enabling the extraction of valuable insights for national security purposes. Likewise, data aggregation involves the amalgamation of information in a way that obscures individual details, striking a balance between the need for comprehensive intelligence & safeguarding personal privacy.

Crucially, finding this equilibrium requires a delicate balance between surveillance capabilities & the protection of individual rights. Governments must employ AI technologies judiciously, ensuring that the scope & intensity of surveillance measures are proportionate to the security threats at hand. Implementing stringent oversight & adherence to legal frameworks becomes paramount in preventing overreach & abuse of surveillance capabilities.

The ethical deployment of AI technologies involves continuous efforts to refine & optimise these techniques, acknowledging the evolving nature of both technology & privacy expectations. By minimising intrusion through responsible use of anonymisation & data aggregation, Governments can demo a commitment to preserving individual privacy rights while still effectively addressing national security concerns. This approach not only upholds ethical standards but also fosters public confidence in the responsible & respectful deployment of AI in the service of safeguarding collective security.

Independent Oversight.

The implementation of Independent oversight mechanisms is crucial in safeguarding the ethical & lawful use of AI applications for national security. Regulatory bodies or privacy commissioners play a pivotal role in monitoring, evaluating & holding accountable Government agencies & organisations employing AI technologies in this domain.

Independent oversight ensures that AI applications are subject to rigorous scrutiny, providing an external check on potential abuses of power. These oversight bodies act as a counter balance, helping prevent overreach & misuse of AI for surveillance or intelligence purposes. By fostering transparency & accountability, independent oversight enhances public trust in the responsible deployment of AI in national security efforts.

Regulatory bodies or privacy commissioners are instrumental in assessing the compliance of AI initiatives with established legal frameworks & ethical standards. They serve as guardians of individual privacy rights, ensuring that data collection, processing & utilisation adhere to defined parameters. If any breaches or misconduct are identified, these oversight mechanisms have the authority to inv, recommend corrective actions & if necessary, impose sanctions.

Furthermore, independent oversight contributes to the ongoing refinement of policies & practices. Through regular evaluations & recommendations for improvement, these bodies help adapt regulations to the evolving landscape of AI & privacy concerns. This adaptability is crucial for ensuring that oversight mechanisms remain effective in addressing emerging challenges & technological advancements.

In summary, the implementation of independent oversight mechanisms is a fundamental safeguard in the responsibility & lawful use of AI for national security. These bodies serve as guardians of privacy, promoting transparency, accountability & adherence to ethical standards, ultimately fostering public confidence in the ethical deployment of AI technologies in the service of national security objectives.

International Cooperation.

International cooperation is paramount in effectively addressing the challenges posed by the use of AI in national security. Collaboration between nations becomes essential to harmonise standards & regulations, creating a cohesive & globally accepted framework that mitigates potential conflicts arising from divergent approaches to AI governance.

The multifaceted nature of AI applications in national security demands a unified understanding of ethical considerations, legal boundaries & the protection of individual rights on an international scale.

Collaborative efforts facilitate the development of common standards, norms, & best practices, fostering a shared commitment to responsible AI use. This harmonisation helps prevent discrepancies in approaches, ensuring a level playing field & minimising the risk of conflicting regulations that could impede international cooperation.

Moreover, shared standards enhance interoperability among nations, allowing for seamless collaboration in addressing transnational security threats. Consistent regulations promote the responsible exchange of information & intelligence, facilitating joint efforts to comb emerging challenges such as cyber threats, terrorism & other global security concerns.

International cooperation also promotes trust & understanding among nations, as collaborative initiatives demo a commitment to collective security without compromising individual sovereignty. Engaging in dialogue & sharing expertise enables countries to learn from each other's experiences, contributing to the development of more effective & ethical approaches to AI in national security.

By fostering collaboration, nations can collectively navigate the ethical & legal complexities surrounding AI, bldg a foundation for responsible & accountable use in the pursuit of national security objectives. Ultimately, international cooperation in the realm of AI governance establishes a framework that transcends geopolitical differences, fostering a more secure & interconnected global landscape.

Technological Safeguards.

The integration of technological safeguards is imperative in preserving the delicate balance between the right to privacy & national security concerns when deploying artificial intelligence (AI) systems. Privacy-enhancing technologies include secure encryption & robust authentication measures; play a pivotal role in fortifying the protection of sensitive data & restricting access exclusively to authorised individual.

Secure encryption standards as a fundamental technological safeguard, transforming data into an unreadable format that can only be deciphered by individual possessing the appropriate decryption keys. By implementing end-to-end encryption, Governments & organisations can safeguard sensitive information from unauthorised interception, ensuring that even if data is accessed, it remains unintelligible without the requisite cryptographic keys.

Additionally, robust authentication measures bolster the security of AI systems by verifying the identity of users. Multi-factor authentication, biometric verification, & other advance authentication protocols enhance the reliability of access controls. This ensures that only authorised personnel can interact with & manipulate sensitive data, reducing the risk of unauthorised breaches.

These technological safeguards not only protect individual privacy but also contribute to the overall integrity of national security efforts. By fortifying the confidentiality & authenticity of data, Governments can confidently leverage AI for intelligence, surveillance & other security applications without compromising individual rights. Moreover, the deployment of such technologies instills confidence in the public, Assuring them that their sensitive information is being handled with the utmost care & security.

In conclusion, incorporating privacy-enhancing technologies constitutes a critical aspect of responsible AI deployment in the realm of national security. These safeguards are instrumental in upholding privacy rights while empowering Governments to harness the benefits of AI for safeguarding national interests in an increasingly interconnected & data-driven world.

Public Awareness & Education.

Public awareness & education are foundational elements in navigating the complex intersection of

artificial intelligence (AI) & national security. Effectively communicating the implications & safeguards associated with these technologies serves to demystify AI, fostering a more informed & accepting public discourse.

Educating the public about the implications of AI in national security involves providing clear information on how these technologies are utilised, the objectives they serve & the potential impact on individual privacy. This transparency is essential in bldg trust & dispelling misconceptions, ensuring that citizens are equipped with accurate knowledge to engage in constructive discussions about the trade-offs between security measures & personal freedoms.

Furthermore, awareness campaigns can highlight the safeguards & ethical considerations embedded in AI deployment for national security. Communicating the existence of legal frameworks, oversight mechanisms, & privacy-enhancing technologies reinforces the commitment to responsible use. This understanding empowers the public to hold Governments & organisations accountable for ethical AI practices & ensures that concerns about privacy rights are addressed proactively.

Education also plays a vital role in mitigating unfounded fears or misconceptions surrounding AI. By providing accessible & comprehensible information, individual can better appreciate the potential benefits of AI in enhancing national security while being cognizant of the safeguards in place to protect their privacy.

In summary, public awareness & education are instrumental in cultivating an informed & engaged citizenry. A well-informed public not only contributes to a more nuanced & bald public discourse but also plays a crucial role in holding policymakers accountable, thereby influencing the responsible & ethical deployment of AI technologies in the realm of national security.

Regular Review & Updating.

The dynamic landscape of artificial intelligence (AI) & national security mandates a commitment to regular review & updating of policies & frameworks. The rapid pace of technological advancements necessitates continuous evaluation to ensure that regulations remain both relevant & effective in addressing emerging challenges & opportunities.

Periodic reviews serve as a proactive measure to assess the evolving nature of AI & its applications in national security. These assessments allow policymakers to identify gaps, vulnerabilities, or potential areas for improvement in existing frameworks. Moreover, they enable the integration of new insights & lessons learned, ensuring that policies are adaptive to the changing technological landscape.

The iterative process of review is particularly crucial in addressing ethical considerations & privacy concerns associated with AI. As societal norms & expectations evolve, policies must be updated to reflect these changes, ensuring that ethical standards are upheld & that the protection of individual rights remains a priority.

Additionally, the review process allows for the incorporation of feedback from various stakeholders, include the public, industry experts & advocacy groups. This inclusive approach ensures that a diverse range of perspectives is considered, leading to more comprehensive & effective policies.

By committing to regular reviews & updates, Governments can demo a responsiveness to the ethical, legal, & societal implications of AI in national security. This adaptability is essential for maintaining public trust, addressing concerns in a timely manner, & fostering an environment in which AI technologies are deployed responsibly & ethically to safeguard national interests. Ultimately, the process of continuous review & updating ensures that policies keep pace with the evolving nature of AI, striking a balance

between innovation, security & the protection of individual rights.

Emergency Circumstances.

In times of emergencies or exceptional circumstances, the delicate balance between the right to privacy & the imperative of national security may necessitate distinct considerations. While the protection of individual rights remains paramount, acknowledging the unique challenges posed by emergencies is crucial for maintaining public safety & responding effectively to urgent threats.

In such circumstances, temporary & proportionate measures may be warranted to address imminent risks or crises. Governments may need to employ advance surveillance technologies or collect & analyse data at an accelerated pace to identify & mitigate threats swiftly. However, these measures must be strictly temporary, limited to the duration of the emergency & directly proportionate to the severity of the situation.

Crucially, oversight mechanisms become even more critical during emergency circumstances. Independent oversight bodies or regulatory authorities should play an active role in monitoring & evaluating the implementation of emergency measures. This oversight helps ensure that exceptional powers granted for national security purposes do not lead to unwarranted & prolonged intrusions into individual privacy.

The principle of transparency becomes equally important during emergencies. Clear & open communication about the nature, scope, & duration of emergency measures helps build public understanding & trust. Governments must provide reassurance that these measures are a response to specific & immediate threats, with a commitment to restoring normalcy & privacy protections once the emergency subsides.

In summary, while recognising the need for flexibility during emergencies, it is imperative that any adjustments to the balance between privacy & national security are temporary, proportionate, & subject to robust oversight. Striking this delicate balance ensures that extraordinary measures are deployed responsibly & ethically, safeguarding both individual rights & collective security during times of crisis.

Achieving equilibrium between privacy & national security in AI demands ongoing dialogue, collaboration, & adaptability. This dynamic balance relies on transparent legal frameworks, ethical practices, & technological safeguards. Governments must engage in continuous communication with the public, fostering trust through clear explanations of AI applications & privacy protections. Collaboration between nations is essential to harmonise standards, preventing conflicts & promoting a unified approach. Adaptability is crucial in navigating technological advancements & evolving threats. Ultimately, a steadfast commitment to protecting individual rights, coupled with responsive governance, ensures the responsibility & ethical use of AI for national security without compromising personal freedoms.

CONCLUSION

Artificial Intelligence is ever growing technology and many countries are focusing in this domain to effectively dominate this rapid growing technology. This tech is still in its nascent stage and many experiments and breakthroughs in this arena are constantly emerging. India as a nation has been proactive in this and we have made considerable development. The roadmap of our nation is clear but still a lot of development is necessary. We have allocated funds and many of the systems and tech are in development or testing phase. The main challenge in this race is the ethical side of employment of these systems.

We need to understand that until now machines helped us to do our tasks and we were the decision makers,

but soon this will be transferred in hands of intelligent systems where we may have little or no control. To obviate a chance of possible mishap of atrocity we have to act proactively while still in designing stage itself. We have to take necessary steps wherein we ensure the development, responsibility and accountability of such tech. We need to thoroughly understand the models and its functioning and device ways to keep a track of decisions made by such intelligent systems empowered by AI.

It is also seen that there is a need to create a International body to devise rules and regulations in the ethical arena and have means of implementing the same. All nations need to understand the seriousness of this tech and implement the international laws with true spirit. In India we need to create a watchdog organisation that regulates and enforces these ethical considerations.