

AI and future of warfare

①

① Introduction

② AI and its history

③ How AI shapes future of warfare.

a) AI-developed autonomous weapons can operate per a pre-assigned objective without a human operator

b) AI-generated deepfakes are used by countries to weaken their enemies by creating civil unrest, violence and confusion

c) Face recognition system uses AI and used in war for the location and hideouts of enemy

d) During the fog of war, AI helps in taking speedy and informed decision by analyzing the situation and social media posts and trends

e) AI enhances the effectiveness of cyber attack to cause maximum damage to the rival

f) AI can enhance efficiency of early warning and radar system by improving detection accuracy, predictive analysis and situational awareness

④ Threats posed by the use of AI in Warfare

a) Autonomous weapons can make error and lose control that can lead to mass destruction

b) Error can occur in early warning system leading to launching a pre-emptive strike

c) Can give rise to AI Arm Race between nations that will lead to

(2)

global instability.

d) There are ethical concerns regarding the use of AI in warfare

(5) Measures needed to mitigate the threats arising from AI use in warfare

a) Establishing global agreements and regulations on the use of AI in warfare

b) Ensuring human decision-making and oversight in AI-driven systems used in warfare

c) Implementing robust cyber security measures to prevent hacking of AI systems used in warfare

d) Spreading education and awareness about the possible consequences of using AI in warfare

(6) Conclusion

With the evolution of humans and technological advancements, warfare has also seen an upgrade in its character - from daggers and hammers in the Stone Age to swords to bows and arrows to catapults.

The invention of gunpowder in China revolutionised the weaponry followed by the development of machine guns, missiles and nuclear weapons. Now, artificial intelligence is changing the future of warfare by bringing autonomy to the weaponry and enhancing the efficiency of other war tactics. Autonomous weaponry is a weapon system that requires no supervision or confirmation before executing its tasks. All the major powers are working rigorously on the deployment of artificial intelligence in warfare. Many countries have introduced autonomous weapons to their weaponry that operate without a human operator.

AI developed deepfakes are used by countries to weaken their enemy by creating civil unrest, violence and confusion. Similarly,

Face recognition and target identification systems are used for predicting the location and hideouts of enemy. Likewise

AI is used to enhance the effectiveness of cyber attacks to cause maximum damage to the rivals. Moreover, AI

is used to enhance early warning system by improving detection accuracy.

and predictive analysis. The use of AI in warfare has resulted in certain threats to humanity and society. The autonomous weapons can make errors that can lead to loss of control thereby causing destruction. Similarly, errors in early warning system can lead to launching a pre-emptive strike. In addition to this, the communication between the autonomous weapons and their human operator can be disrupted by the rival by waging electronic warfare that can jam the weapons. Additionally, misidentification of target can occur resulting in killing civilians and even people. In the same way, AI arm race between the nations can lead to global instability.

There is a dire need to address the threats emanating from the use of AI in warfare by setting international regulations and treaties and strengthening accountability mechanism. The use of artificial intelligence in warfare has revolutionized the character of war. However, certain threats have been posed which should be addressed by taking pertinent measures.

The concept of creating intelligent machines has ancient roots in myths and legends, such as the ancient Greek myth Talos. However, the word "artificial intelligence" was first coined by

John McCarthy in 1956. The development of AI can be traced back to early AI programs like the Logic Theorist, designed to mimic human problem-solving using symbolic logic. Notable milestones include the creation of expert systems like Dendral and the introduction of the term "artificial intelligence" at the Dartmouth Workshop in 1956. The field experienced periods known as "AI winters" characterized by reduced funding and enthusiasm. However, the resurgence of AI was fueled by advancements in machine learning, neural networks, and the availability of large datasets.

Artificial intelligence encompasses tasks executed by programs or machines that would typically require human intelligence for their completion. It involves the field of science and engineering dedicated to crafting machines that exhibit intelligence, particularly in areas like visual perception, speech recognition, decision-making, and multi-lingual translation, mirroring human capabilities. AI is the emulation of human cognitive processes using machines, particularly computer systems, encompassing facets such as learning, reasoning, planning, self-correction, problem-solving, knowledge representation, perception, motion, manipulation and creativity. AI is closely linked with machine learning and deep learning. Machine learning leverages algorithms to uncover

patterns and derive insights from data it processes. Deep learning, a subset of machine learning, brings AI nearer to the aspiration of enabling machines to think and function as closely to human as possible. AI has become an integral part of human daily life actively shaping the future.

Autonomous Weapons use AI to operate on and are increasingly used by countries in warfare. They use AI, sensors and other technologies to perform tasks that traditionally require human decision-making. They range from armed drones and unmanned aerial vehicles (UAVs) to ground-based robots and naval vessels. Autonomous weapons carry out missions autonomously such as surveillance, reconnaissance and combat operations, without direct human control. These weapons, once activated can fly for hours till they acquire a target and destroy it. It becomes very difficult for the opponent to fight them and take counter measures. They have completely changed the landscape of warfare. Many leading powers of the world have been using autonomous weapons in war. The use of autonomous weapons in war has long history. Israel was the first country putting them to practice in 1970. The U.S. used unmanned reconnaissance aircraft in live fire in Gulf War of 1991.

It is due to advancement in AI that countries are using autonomous weapons in war. Therefore, AI governed autonomous weapons will be used by more countries in warfare with the advancement in artificial intelligence.

Similarly, AI-generated deepfakes can be used in warfare to weaken the enemy by creating civil unrest, violence and confusion. Deepfakes are images, videos, or audio which are edited or generated using artificial intelligence tools that may depict real or non-existent people. It can be used for various purposes against rivals. It can lead to violence against minorities when used to target a specific religion by insulting its leaders or pious books. It can be used for political propaganda to spur communal riots. Moreover, deepfakes are deployed to falsify order from enemy's military leadership to create confusion and cause damage to army. For instance, Russia released an AI-edited video in which Ukrainian President Volodymyr Zelensky could be seen announcing a surrender to Russia. This created confusion in Ukrainian government and its public. Thus, AI-edited deepfakes can be used in war to weaken the enemy.

Moreover, AI developed face recognition system can be used in war for predicting the location and hideouts

of enemies. Face recognition system is a technology that uses AI to detect faces in images or videos and then compare them with stored templates to identify or verify individuals. This system can selectively target a specific person without collateral damage. It has been widely used against terrorists by many countries. AI could help identify and predict the location and hideouts of terrorists by putting together and evaluating a number of factors and pieces of information like terrain, population composition, terrorists communication and other intelligence input. This helps to determine their surfacing patterns and aid in their targeted killing. AI-powered drones have been used by the U.S. in various countries like Pakistan and Afghanistan against terrorists like Al-Qaida and ISIS-MQ-9 Reaper, one of the drones used by the U.S. against terrorist in Pakistan, uses AI for target recognition, tracking and autonomous navigation. Therefore, AI can be used in warfare due to its facial recognition system for predicting location and hideouts of enemies.

Likewise, during the fog of war, AI can be used for taking speedy and informed decisions to fight enemy vigilantly. AI can help in this regard

by analysing the situation and using social media trends and contents. Speed of decision-making during war was greatly influenced by the AI based system. AI based system analyzes the situation during war by processing vast amounts of data received from various sources such as sensors, drones and satellites. It then predicts outcomes of different courses of actions. After all this, AI based system takes speedy and accurate decision within fraction of time. Also, AI can help in speedy decision-making during war by analyzing social media posts to gauge public sentiments, predicting potential conflicts and identifying trends and patterns in social media conversation to anticipate enemy movements and plans. One such AI based system is Bore Manor Research's (Bore) "STARTLE" machine situational awareness software, which would make informed decision as well as aid in decision-making. Therefore, AI can be in fog of war which will ensure speedy decision making.

Additionally, AI can be used to enhance the effectiveness of cyber attacks to cause maximum damage to the rival country. A cyber attack is an unauthorized and malicious attempt launched from anywhere in the world to access, disrupt or damage computer systems, networks or electronic data of an individual.

organization or a government. AI can help enhance the effectiveness of cyber attack by collecting and analyzing vast amount of data to identify vulnerabilities and targets. Similarly, AI can predict enemy cyber defenses and identify the most attack vectors thereby strengthening the cyber attack on an enemy. It can make cyber attack faster and efficient because it can automate the exploitation of the vulnerabilities. Also, AI can aid in the creation of sophisticated malware that can evade detection and adapt to changing environment. In 2015, Russia used BlackEnergy, a type of malware, in the attack on Ukraine's power grid, causing power outages. AI was used for navigating and disrupting the system. Thus, AI can enhance the effectiveness of cyber attack conducted against rivals.

Last but not the least, artificial intelligence can be employed in warfare to enhance early warning and Radar system to take proactive measures against enemy's attack. Early warning and radar system is a network of sensor and detection systems used to identify and trace potential threats, such as incoming missiles, aircrafts, at a distance, enabling timely response. AI can enhance the functioning of this system because it can analyze sensor data more accurately, detecting threats

earlier and reducing false alarm. Also, AI can predict target trajectories, improving tracking accuracy and enabling more effective response. AI can process large amount of data in real-time thereby enabling faster response. Israel's Iron Dome defense system uses AI, and it successfully intercepted around 99 percent of the incoming missiles launched by Iran on April 13, 2024. This shows that now AI can make defense system stronger than traditional one. Thus, AI can make early warning and radar system of a country more efficient in war against enemy.

The use of AI in warfare poses certain threats. Autonomous weapons can make errors and lose control that can lead to mass destruction and outbreak of conflict. These weapons can make errors due to sensor failure that leads to misidentification of the target. Similarly, software glitches and data corruption can lead to misinterpretation of the situations. Cyber attacks can also compromise autonomous systems leading to loss of control. There is possibility of loss of communication between system and human operator that results in loss of control causing damages. This can lead to large-scale destruction, attacking own forces or civilians and autonomous responses leading to

further conflicts. A report by the International Committee of the Red Cross (ICRC) noted that autonomous weapons have been involved in at least 10 incidents resulting in civilian casualties. Therefore, AI-developed autonomous weapons pose a threat because they can make errors and lose control causing mass destruction.

Similarly, AI-deployed early warning and radar systems can make errors that can lead to launching a pre-emptive strike. These systems use sensors for data collection for target identification. Any fault or error in sensors can degrade sensor data can lead to inaccurate tracking or incorrectly identifying friendly targets as hostile and failing to detect actual threats. They are also prone to cyber attacks that can lead to manipulated or false readings. There is risk of nuclear war due to errors in these system which can lead to mass destruction and world war III. For instance, in 2003 Iraq war, the U.S. automated system of surface-to-air missiles Patriot misidentified a friendly aircraft as an enemy aircraft that led to the death of own Pilot. Likewise, in 2019, a Russian S400 system failed to intercept a Ukrainian drone, leading to friendly fire incident. Thus, the use of AI in early warning and radar system is prone to error leading

to negative consequences.

In addition to this, there is a risk of artificial intelligence arm race between major powers that can lead to global instability, chaos and peace destruction. Arm race is a situation where two or more countries or entities compete to acquire more powerful and advanced weapons, military technology, and capabilities than their opponents. This has several negative consequences as this can lead to increased military spending compromising funding for human capital development. In order to keep pace with and maintain balance of power to make defence system updated, when one major power will make advancement in deployment of AI in warfare, the other major will also do its best for making advancement in AI deployment in warfare. This will lead to heightened tensions between major powers and proliferation of weapons of mass destruction that can cause unintended accidents. There will be decreased international cooperation and diplomacy that can lead to job displacement and economic disruption. In 2021, the U.S. Department of Defense allocated \$874 million for AI-related research and development. China's "AI by 2030" Plan aims that China will

become world leader in AI by 2030, surpassing the U.S. The government has pledged to invest \$150 billion in AI development. Therefore, the deployment of AI in warfare can lead to AI arm race.

Lastly, there are ethical concerns over the use of AI in warfare that involve issues of accountability, human rights and the moral nature of autonomous decision-making. Autonomous lethal weapons can select and engage target without human intervention which raises concerns about whether machines should be allowed to make life-or-death decisions. Another ethical dilemma is the potential removal of human judgement from the use of lethal force that may lead to decisions made without moral and contextual understanding that only human can provide. Similarly, with AI system making decision, it becomes unclear who is responsible when things go wrong. Misidentification can lead to killing of non-combatant which is unethical. AI technologies in military setting can be used for mass surveillance which may infringe on individual rights and freedom. In 2021, an experiment by the U.S Air Force saw an AI-powered drone beat a human fighter pilot in a dogfight simulation. While the AI outmaneuvered the pilot, the event sparked ethical concerns about AI-controlling real-world lethal systems in warfare without human oversight. Thus, use of AI in warfare presents ethical concerns.

In order to mitigate the threats emanating from the use of AI in warfare, there is a need to establish global agreements and regulations on AI development and its use in warfare. It requires collaboration among nations, international organization, and stakeholders. All major powers should cooperate in this regard to make the globe a peaceful place. Principles and guidelines for the responsible use of AI in warfare should be devised and implemented. Technical standards should be for AI system design and deployment. Internal standards should be followed by AI developers and industry leaders in producing autonomous weapons and other warfairs. A new international treaty should be negotiated which will only address AI use in warfare. Certain countries have already taken steps in this regard. For instance, the U.S. DoD has established guidelines for the autonomous weapon systems and has set certain standards. ECW can be expanded to address AI-powered weapons. Therefore, major powers should cooperate to establish global agreements and regulations on the use of AI in warfare.

Similarly, there is a need to ensure human decision-making and oversight in AI-driven systems and weapons used in warfare. Clear guidelines and protocols should be established for this purpose.

These systems and weapons must have human monitor and intervening facility where human can intervene when needed.

They should be designed in such a way that human can set objectives and constraints, and can make final decision.

This will escape the risk due to errors in such system and will prevent loss of lives and other destruction.

Also, proper training and education should be provided to the personnel on AI system capabilities and limitations.

According to ICRC, 94% of AI experts believe human oversight is essential for autonomous weapons.

Human oversight in these systems will decrease the chances of pre-emptive strike and possible nuclear conflicts.

Therefore, human oversight should be ensured in AI-driven systems and autonomous weapons used in wars to prevent negative consequences.

Moreover, robust cyber security measures should be implemented to prevent hacking of AI systems and weapons used in warfare.

Cyber security refers to practices, technologies and processes to protect digital information, computer systems, and networks from unauthorised access, use and destruction.

Secure coding practices should be implemented and regular code reviews and testing should be carried out.

AI systems should be protected with firewalls, intrusion detection and encryption. Also, access to these systems should be given to only authorized personnel and multi-factor authentication should be used. Cyber security training be provided to the personnel associated with these systems and response plan for AI-related security incidents should be implemented. International AI cybersecurity guidelines, for instance NATO's AI Cybersecurity Guidelines, should be followed. All this will make cybersecurity stronger and will prevent AI-system hacking thereby mitigating the threat with hacking of AI-systems used in warfare. Thus, it is advisable to implement robust cyber security measures to prevent hacking of AI-systems used in warfare and prevent devastating effects.

Lastly, education and awareness about the possible consequences of using AI in warfare is required for promoting responsible development and use of AI in warfare. Policymakers and military personnel should be provided training and workshops on AI's implication in warfare. Public events, campaigns and media outreach are necessary for raising awareness among general public about AI's used in warfare and its consequences. Online courses and tutorials should be developed and podcasts should be conducted to provide insights and guidance.

Documentaries and films should be produced showcasing AI's implications in warfare. All this will make AI developers to design weapons that are least harmful to the civilians and to make sure they are not violating human rights. Policymakers and military personnel will make informed decisions regarding AI's implication in warfare. It can also prevent accidental escalation reducing unintended consequences. It will reduce concern and promote trust of general public. Therefore, education and awareness about AI use in warfare is necessary to mitigate its negative consequences.

To conclude, it can be said that artificial intelligence has completely changed the landscape of future warfare. Certain threats have been posed by the use of AI in warfare which can be mitigated by taking robust measures. AI developed autonomous weapons has revolutionized the warfare as they can operate on certain pre-assigned objective without human operators. Certain countries use AI-generated deepfakes against enemies to weaken them. Similarly, face recognition system uses AI and can be used to identify and locate enemy. Moreover, AI enhances the effectiveness of cyber attacks to cause maximum damage to the

critical. Certain threats are associated with the use of AI in warfare. Autonomous weapons can make error and lose control thereby leading to mass destruction. In the same way, errors in early warning system can lead to launch a pre-emptive attack. Likewise, this can give rise to AI arms race between nations that will lead to global instability. Establishing global agreements and regulations on AI development and its use in warfare can help mitigate these threats. Similarly, ensuring human decision-making and oversight in AI driven systems and weapons can help in this regard. Exploitation of the use of AI in warfare is possible if these measures are taken in true letter and spirit.