International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

The Rise of Robotics: Artificial Intelligence as a Weapon

Aryan Sanjeev[1], Pari Paliwal[2]

[1]2nd Year, B.Tech Undergrad Amity School of Engineering &Technology, Amity University Noida, India
sanjeevaryan2011[at]gmail.com

[2]2nd Year, B.Tech Undergrad Amity School of Engineering &Technology, Amity University Noida, India
diyapaliwal10[at]gmail.com

Abstract: ***Technological advancement has devolved into a rat race. Artificial intelligence (AI) is rapidly becoming the centre of the global power play in the race to lead the emerging technology race & the futuristic warfare battleground. We adore the fact that we can unlock our phones with our faces & that Amazon can anticipate our needs. From a smart vacuum that can learn floor plans to "Killer Robots" that can revolutionise the battlefield, AI has both mundane & extraordinary applications. While AI applications in healthcare, education, logistics, & agriculture help people develop, its military applications can make war more lethal. The development of autonomous weapons systems (AWS) is advancing rapidly across many nations, & this increase in the weaponization of artificial intelligence appears to be a highly destabilizing development. The use of machines to harm one's adversary has a history that rivals that of humanity itself. However, recent advancements in automation & artificial intelligence may, for the first time in recorded history, transfer control of violence from humans to machines. This possibility has sparked a heated debate on ethics & morality in a variety of national & international forums concerning the use of such machines. The primary goal of this conceptual paper is to alert the lay reader (rather than the expert or practitioner) to the dangers posed to global communities by nation-states' continued efforts to merge Artificial Intelligence (AI) with lethal autonomous weapon systems (LAWS). Human-armed inter-state warfare is primarily regulated under International Humanitarian Law (IHL). However, LAWS provide an especially strong threat to IHL, owing to the former's ability to completely replace the human person (as the administrator of violence), calling into doubt the validity of the basic adjective "humanitarian" upon which the entire superstructure of IHL is founded.***

Keywords: Artificial Intelligence, Autonomous Weapon Systems (AWS), International Humanitarian Law (IHL), Lethal Autonomous Weapon Systems (LAWS), Unmanned Underwater Vehicle (UUV), Cybersecurity, Robotics, Warfare

1. Duality of Artificial Intelligence

Due to AI's dual nature, software created to improve our quality of life may also be used against us. The algorithm used to determine which junk email should be forwarded to our spam folder, for example, can also be utilised by malware software. In order to detect targets with rifles, object-oriented software is being tested with the capability that lets us unlock our phones with our faces. Similar to this, the same weapons that are used in conflict to hit the target precisely & save lives might also kill people who are deciding their own fate. Particularly when technology is utilised for military purposes, the AI paradox of its dual nature is causing grave concern. [2]

With breakthroughs in machine learning, computing power, international investment, & data availability, AI has potentially universal uses, which increases the security issues involved enormously. Furthermore, because AI integration is undetectable to the human eye, the potential to cognitize anything & everything significantly transforms the security picture. AI's automation & intelligence bring both promise & the potential for disaster. [2]

Since AI has the potential to be integrated into nearly every product & service in cyberspace, geospace, & space (CGS), this developing cognitive ability significantly transforms the security situation for mankind across CGS. Technology, computing power, programming languages, computer code, encryption, information, big data, algorithms, & investment all have dual applications right now. [3]

As digital data in cyberspace becomes contested commons, the democratisation of big data ushers in a fundamentally new world order. This new world order ushers in a new reality in which anybody, from anywhere, may access digital data & use it for the good or ill of humanity. Today, any individual or entity with a desire to access big data & data science capabilities can utilise it for whatever intelligence, automation, surveillance, & reconnaissance they want to achieve, regardless of their education, background, social status, or goals in society. [3]

Should the democratisation of digital data go unchecked, with no accountability or obligation, given that data is required to develop most AI systems? [3]

2. Weaponized Artificial Intelligence

While AI is clearly making our lives easier, the same technology is increasingly being militarised. AI weaponization refers to the intentional use of AI to cause harm to humans by incorporating it into national militaries' systems & tools. Aside from previous revolutionary innovations, it is feared that weaponized AI would disrupt world security & peace. [2]

When nations accelerate their efforts to achieve a competitive advantage in research & technology, greater weaponization of AI is unavoidable. As a result, it is necessary to imagine what an algorithmic war of the future would look like, because developing autonomous weapons

systems is one thing, but employing them in algorithmic conflict with other states & against other humans is quite another. As stories of complex algorithmic systems supporting more & more facets of warfighting across CGS emerge, the truth is that AI commoditization is already a reality. Automated warfare (cyberwarfare), as seen in cyberspace, has already begun, with anyone & everyone as a target. [4]

Weaponized AI is referred to as "Algorithmic warfare" by the US Department of Defense (DoD), & the true goal of establishing JEDI (Joint Enterprise Defense Infrastructure: the US Department of Defense) was to weaponize AI. In April 2017, the Pentagon announced the "Maven" project. Maven was the military's first attempt to use AI in warfare, with the goal of enhancing the precision of existing weapons such as drones by incorporating AI. Machine learning was initially used to scan drone video footage. This scan also assisted in identifying individuals, vehicles, & locations that might be worth bombing. However, Google's staffs were not enthusiastic about the initiative. Many staff quit, & over 3000 employees signed a petition in protest of their company's support to the research, fearing that it might lead to the use of artificial intelligence against human survival. [2]

In his study published in 2019, Vadim Kozyulin says that private businesses such as IBM, Amazon, & Microsoft developed most AI tools & submitted them to the military. He goes on to say that Combat Robots intrigue the Russian Ministry of Defense. Combat robots are multi-functional machines with sensors, a control system, & actuation devices. They have human-like behaviour & can carry out combat missions just like humans. As a result, weaponized AI is driving us to autonomous warfare in which Lethal Autonomous Weapons Systems (LAWS) will serve as soldiers. [2]

Lethal Autonomous Weapon Systems

In the military industry, AI is being used to create & deploy completely autonomous weapons systems at a rapid speed. Once activated, such autonomous weapons may detect, identify, attack, & kill human targets on their own without human intervention. These weapon systems, known as "Lethal Autonomous Weapons Devices" (LAWS) or "Autonomous Weapons Systems" (AWS), contain both lethal & less-lethal systems & have the potential to change the entire character of warfare. [2]

Autonomous & Semi Autonomous

Systems at Present

As AI advances, it carries with it the tantalising prospect of eliminating the need for the shaky communication ties that bind commanders to their troops. Of course, killer robots are not yet the norm; but, there are precursors that clearly demonstrate the pattern of increasing autonomy. The Israeli "Harpy" Loitering Bomb, for example, can linger in the air for extended periods of time, scanning for hostile radar signals.[1] When they are discovered, it uses controlled self-destruction to attack & destroy the enemy radar. In the 1990s, Israel sold 100 Harpys to China for $55-70 million, marking a watershed moment in US-Israeli relations. Some businesses in Slovakia & the United States have also developed loitering munitions.[2] South Korea employs an autonomous shooting sentry gun known as the SGR-A1. SGR-A1 is an AI-enabled robot 'infantry guard' built in the early twenty-first century & successfully tested over a decade ago (in 2006). It has been deployed on the border between North & South Korea, & it is described as an armed sentry who never sleeps & whose attention is unwavering. It is armed with an automatic rifle & a grenade launcher & can detect humans using infrared sensors, although it requires the approval of a human operator to fire. [1]

Milrem Robotics' THeMIS (Tracked Hybrid Modular Infantry System) robot was created in Estonia. THeMIS has a mobile body that is mounted atop tank treads. On top is a remote-weapon tower with machine guns. This robot also has cameras & software to track the targets. This target-tracking software is set up to allow the tower to pursue persons or objects. Milrem ensures that THeMIS will remain a human-controlled system.

In cases where human operators can be inserted into the loop, the future may see autonomy only in the technological realm rather than in the actual decision-making process. This is more likely to occur in the aerospace & l& sectors, where establishing communications is easier. However, in the marine sector, communications provide a higher difficulty, & the desire to apply AI even for decision-making is very strong. Unlike on l&, the vast oceans lack permanent infrastructure for receiving & sending messages. Surface ships, as a result, have extensive on-board communication suites that allow them to communicate with one another as well as with l&-based authorities. Surface fighters, whether those on l& or in the air, communicate using radio waves. The atmosphere is a good medium for these radio waves to flow through, but water is not. As a result, submerged boats such as submarines are considerably more difficult to communicate with. Subsurface vessels communicate primarily using underwater acoustic systems, which cannot transmit through air. The air-water communication barrier is substantial, making the subsurface domain a suitable environment for AI deployment. The term "Unmanned Underwater Vessel" (UUV) has already become synonymous with the expression "Autonomous Underwater Vessel" (AUV), & such vehicles are already being used by many countries for scientific research as well as for purposes ranging from intelligence gathering, surveillance missions, reconnaissance, & mine-countermeasures. The secrecy surrounding naval underwater systems makes it difficult to determine how many countries have UUV capability & to what extent. However, it is well known that the United States, Russia, China, France, Germany, the United Kingdom, China, Israel, & India are among a fast rising list of countries with robust UUV programmes, with AI increasingly being integrated into all such boats. UUVs/AUVs vary greatly in size & shape, ranging from microscopic to very big boats, each with its own set of advantages & limitations. [2]

These AI-enabled weapons were originally created to reduce the threat to humans in military battles; nevertheless, if fully autonomous, they can cause catastrophic damage in autonomous wars. The transition from semi-autonomous

weapons to fully autonomous weapons systems is happening quickly, but it is uncertain when researchers will be able to build a totally lethal autonomous weapon. In the United Kingdom, the Taranis Drone is an autonomous military aerial vehicle that will most likely be completely operational by 2030. This drone is thought to be capable enough to replace Tornado GR4 fighter jets. [2]

Risks of Weaponizing AI

Security Dilemma

For much of human history, the notion & approach to security have essentially centered upon the use of force & the territorial integrity of geospace. As the definition & meaning of security are fundamentally challenged & changed in the world of artificial intelligence, the notion that traditional security is about violence against respective nations in geospace from within or across their geographical boundaries is now outdated & needs to be evaluated & updated. The problems & complexities of emerging AI threats & security have transcended space, ideology, & politics, necessitating a constructive collaborative effort across nations. Collective NGIOA brainstorming is required for an objective assessment of what a threat is & how it might be secured? [3]

Cyber-Security Challenges

In short, algorithms are far from secure—they are vulnerable to errors, viruses, bias, & manipulation. &, because machine learning employs machines to train other machines, what happens if the training data is tampered with or manipulated? While security dangers exist everywhere, linked devices improve the possibility of cybersecurity breaches from remote locations, & security is extremely hard due to the code's opacity. As a result, when AI goes to war with other AI (whether for cyber-security, geo-security, or space-security), the continuous cybersecurity difficulties will add colossal threats to humanity's & the human ecosystem's future in CGS. [4]

Role of Programmers & Programming

Despite these complicated security concerns & the sea of unknowns that await us, the role of programmers & programming, as well as the integrity of semiconductor chips, remains important for the safety & security of the human race. The reason for this is that programmers can define & determine the nature of AWS (at least initially) until AI learns to programme itself.

Furthermore, because AWS is concentrated on software, who should bear responsibility for faults & tampering with AWS system design & use? That takes us to the crux of the issue: if & when an autonomous system kills, who is liable for the killing, whether justifiable or not? [4]

AWS & Human Rights

The development, deployment, & use of AWS raise serious concerns for human rights, potentially jeopardising the right to life, the prohibition of torture & other inhumane, cruel, or degrading treatment or punishment, & the right to individual security, as well as potentially jeopardising other human rights. [1]

The war between Armenia & Azerbaijan, which ended in November 2020, is an instructive example of the employment of autonomous systems in battle. Drone attacks, which killed Armenian & Nagorno-Karabakh soldiers & destroyed tanks, artillery, & air defence systems, gave Azerbaijan a decisive win in the 44-day battle. [1] However, this new aspect of the two countries' military struggle transformed it from a violent, bare-knuckled ground fight into a lethal but enticing game of hide-&-seek against an all-too-patient - & frequently invisible - airborne non-human enemy. Hundreds of people died in less than two weeks, causing major damage to more than 120 residential & institutional structures in the town. The drone strikes caused the evacuation of approximately 6,000 inhabitants, with the majority of women & children seeking sanctuary outside. Nobody should be arbitrarily deprived of life, according to a core principle of international human rights law. [1]

AWS would need to be able to assess the level of threat of death or serious injury, identify the danger's source, decide whether employing force is necessary to neutralise the threat, be able to recognise & use alternatives to force, be able to set up various forms of communications, & be able to set up police weapons & equipment to take action when necessary in order to have at least the option to carry out policing & law enforcement responsibilities in a legitimate manner.

The multiplicity of issues caused by AI weaponization & autonomous weaponry necessitates rapid action. Many states advocate a wait-&-see attitude due to uncertainty about what AI can accomplish. However, the enormous risks necessitate a cautious approach. Whatever approach is taken, weaponized AI is ultimately leading us to Autonomous Wars, which pose a significant threat to civilization. So, whether we like it or not, we must accept that we have entered the era of algorithms, &, like any other industry, AI is transforming our status in the conflict zone through its use in military applications. [2]

I. Ban on Autonomous Weapons:

A) Legal & MoralObligation

Looking ahead to a dismal future dominated by autonomous weaponry, the United Nations granted the option of imposing an international ban on Killer Robots in 2013. More than 100 experts from the AI community participated in the debate, including Elon Musk from Tesla and Mustafa Suleyman from Alphabet. These leaders signed an open letter arguing that developing lethal autonomous weapons or killer robots would be like opening Pandora's Box, irrevocably changing the character of conflict. They also cautioned that self-driving weapons might usher in the "third revolution in warfare," following gunpowder and nuclear weapons. [2]

In a 2017 report, the "World Commission on the Ethics of Science and Technology" (COMEST) and the "UNESCO Ethics Committee" examined "armed military robotic systems (armed drones)" and "autonomous weapons" in terms of mobility, interactivity, communication, and autonomy capacity to make decisions without external

intervention. According to the paper, legal norms and engineering codes of conduct may apply, and a cognitive robot, in which decision-making is delegated to a machine, involves the duty of designers and manufacturers, as well as the use of the precautionary principle. The report emphasised that the use of AWS would be a violation of international humanitarian law. They violate the fundamental concept that machines should not make life or death choices for humans". The document said, "In terms of technical capability, autonomous robotic weapons lack the key components required to insure conformity with the principles of distinction and proportionality." Though it could be claimed that compliance is possible in the future, such projections are perilous in the face of killing machines whose behaviour in a given situation is stochastic and thus intrinsically unpredictable." [1]

Jody Williams, who campaigned on landmine bans and was awarded the Nobel Peace Prize, was an enthusiastic supporter of the movement to stop killer robots. The goal of this movement was to outlaw lethal autonomous weapons. This campaign's participants included activists, civil society organisations, well-known scientists such as Noam Chomsky, and more than 450 AI researchers. [2]

Employees of digital behemoths such as Google, Microsoft, and Amazon have questioned their companies and raised ethical concerns over the use of AI for military objectives. In 2018, over 170 technology companies, including Google DeepMind and the XPRIZE Foundation, and over 2400 AI and robotic researchers, academics, and engineers signed the Lethal Autonomous Weapons Pledge. This vow said that they will not participate in the development or use of autonomous weapons. Almost 29 countries from the global south have strongly backed a ban on such autonomous weapons, fearing that these devastating weapons may be used against them. On September 12, 2018, 82% of the European Parliament voted in favour of an international ban on AWS having significant human control over dangerous weapon functionalities. [2]

Furthermore, fully autonomous weapons are now the most frightening yet still developing military technology. Under the Martens Clause, such fully autonomous weapons must be closely monitored by specialists, the general public, and states. Martens Clause is an exclusive provision of IHL (International Humanitarian Legislation) that establishes a model of protection for both combatants and civilians when no specific agreement or law on a topic exists. According to the Martens Clause, when there is no international agreement or law on an issue, combatants and civilians must be safeguarded based on regional tradition and humanitarian considerations. As a result, because there is no international law governing their deployment, this legislation applies to totally autonomous weapons. Martens Clause also gives states with key components or moral norms to consider when appraising emerging weapons technology, particularly autonomous weapons. [1]

3. Conclusion

AI is indisputably the future of warfare, and weaponization of AI is the new game. This game features the creation and deployment of lethal autonomous weapon systems (LAWS). Many weapon systems with varying degrees of human interaction are now in operation. However, advances in AI are rapidly heading to autonomous warfare in which AI-enabled weaponry will battle independently against each other without human intervention. AI will very certainly be integrated into weapons systems and utilised to improve the precision, lethality, and destructiveness of military power. Concurrently, constant attention must be paid to the legal, ethical, and strategic debates surrounding human enhancement, including the physical and cognitive development and evolution of military forces, as well as how psychical and cognitive processes may change and evolve as weaponized AI is increasingly integrated into war fighting. [1]

To cut a long tale short, "the AI genie is now out of the bottle". The methods for weaponizing AI are less theatrical, but as terrifying. As weaponized AI has begun to touch our world, there is a tremendous need to find the best ways to govern it effectively in order to avert the feared autonomous wars. Furthermore, if terrorist organisations begin to use AI with malicious purpose, our greatest defence should most likely be an AI offence. [2]

This raises some significant concerns. Is it desirable to weaponize? Should the international community try to control and stop these processes, and what impact would it have on non-military applications of AI? In this regard, the authors believe that the hyperbolic argument over "killer robots" misses the mark. [1]

References

[1] Nair, Shweta. (2021). RISE OF THE ROBOTS: WEAPONIZATION OF ARTIFICIAL INTELLIGENCE. National Maritime Foundation. Retrieved from https://maritimeindia.org/rise-of-the-robots- weaponization-of-artificial-intelligence/
[2] Suhaib, Kanwal. (2021). Autonomous Wars & Weaponized AI. *ThinkML*. Retrieved from https://thinkml.ai/autonomous-wars-&- weaponized-ai/
[3] Pandaya, Jayshree. (2019). The Dual-Use Dilemma Of Artificial Intelligence. *Forbes, Innovation.* Retrieved from https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual- use-dilemma-of-artificial-intelligence/?sh=7e6d0ca96cf0
[4] Pandaya, Jayshree. (2019). The Weaponization Of Artificial Intelligence. *Forbes, Innovation.* Retrieved from https://www.forbes.com/sites/cognitiveworld/2019/01/14/the- weaponization-of-artificial-intelligence/?sh=22d25fad3686