JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER TERRORISM AND AUTONOMOUS WEAPONS – THE RISK OF AI IN WARFARE

Name of the Author – Esha Yadav

Designation of 1st Author- Student at Law College Dehradun

Affiliated to - Law College Dehradun, Uttaranchal University, Dehradun-248007, Uttarakhand, India

Name of the 2nd Author – Mrs. Priyadarshini Tiwari (Asst. Professor)

Designation of 2nd Author – Assistant Professor at Law College Dehradun

Law college Dehradun, Uttaranchal University Dehradun, 248007 Uttarakhand, India

1. ABSTRACT:

Cyberterrorism is a worldwide concern that is often disregarded and undervalued in India. After the United States and China, India has the most "Netizens," or people who utilize the internet. Their over-reliance on the internet made them more vulnerable and converted their animosity into a desire for vengeance, turning them into cyber-warriors, criminals, and enemies of the nation. The majority of Indians are oblivious to the dangers of cyberspace and become victims of online fraud. The globe now has a plethora of options to expand its financial infrastructure thanks to information technology. Cybercrimes are growing every second. The people who use the internet are illiterate and believe that no one is watching what they do. The enormous expansion of the cyber world brought with it the fear of cyber terrorism. Cyberattacks frequently portray psychological health, public confidence, and political views as either deadly or non-lethal. In general, it should be considered that cyberterrorism only impacts the national security framework. Yet, it also has an impact on their mental and cognitive health. The proliferation of cyberterrorism has led to a sharp rise in cyberattacks over the last several years. It has damaged vital command and control systems, nuclear facilities, and caused catastrophic catastrophe. Cyber specialists are attempting to increase the capacity to thwart cyberattacks against critical nuclear plants, commercial and banking systems, defense websites, and government systems.

Autonomous weapons use little to no human intervention to engage and destroy targets. Although fully autonomous weapons are not currently in production, many nations are creating or using systems that are almost autonomous. Even defensive systems will drastically alter how states see war and have a direct impact on trade and the balance of power, even if no government has admitted to fielding autonomous offensive weaponry. The morality of these weapons and their status under international humanitarian law are the subject of a small but fierce global debate. The state of Pakistan and the UN special envoy on extrajudicial murders have both offered arguments in support of a preemptive moratorium on the creation of such weapons, even if a consensus has not yet been established. India should examine this discussion from the perspective of its security requirements. The nation's defenses will be strengthened by autonomous weaponry, which may even be more effective than human soldiers in achieving some strategic goals like thwarting cross-border incursion. India should actively participate in the process of establishing an international regulatory framework and develop autonomous weaponry.

This research aims to give a general review of autonomous weapons' current situation and discuss whether or not they need to be outlawed.

Keywords: Artificial Intelligence (AI), Autonomous Weapons, Cyber Security, Lethal Autonomous Weapon Systems (LAWS), Military artificial Intelligence (MIA), Machine Learning (ML), Weapons of Mass Destruction (WMD)

2. INTRODUCTION:

The extremely advanced autonomous military weapon systems known as LAWS are equipped with a variety of sensor suites and pre-programmed computer algorithms that enable them to independently locate, identify, track, engage, and destroy hostile targets. Once engaged, these weapon systems may destroy targets without the need for additional human assistance.

Therefore, by integrating AI into systems that control weapons without involving people, LAWS on a large scale can change the way that war is fought. Today, the world's top military institutions are experiencing an AI-triggered Revolution in Military Affairs (RMA).

2.1 Concerns about ethics and legality:

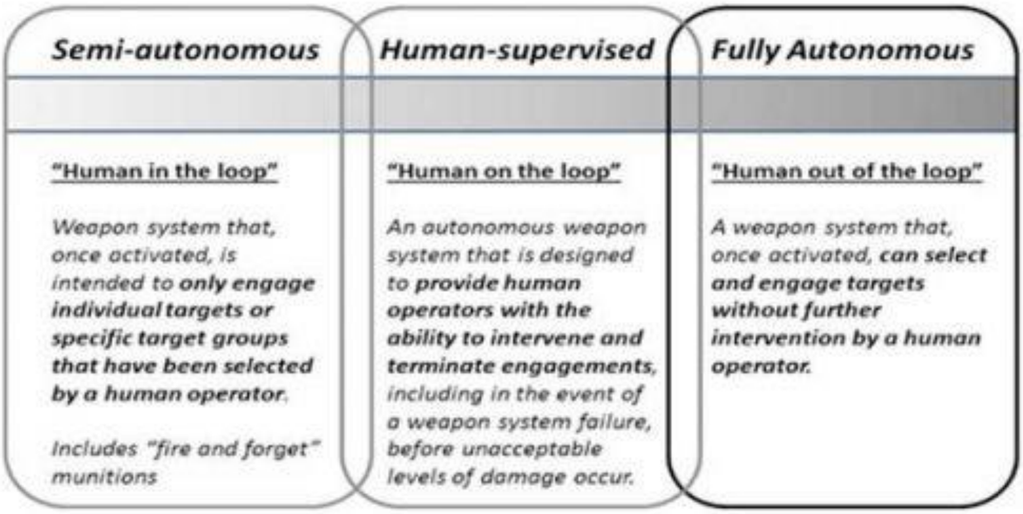
LAWS, also referred to as "killer robots," may be seen as unethical given its lethality and ability to replace humans in making crucial tactical judgments. Deploying and commissioning LAWS presents the biggest challenge: accepting accountability for a misfire. LAWS is an AI-enabled killing machine that is uncontrollable by humans, it presents a number of philosophical, psychological, and legal concerns. As a matter of fact, these weapons possess the capacity to upset the current conventional warfare paradigm.

Human rights advocates are fighting against LAWS because they would be against both IHRL under the UDHR and IHL under the Geneva Convention.

The dissatisfaction among Google workers working on the coveted Pentagon "Project Maven" demonstrates how young people are becoming more conscious of LAWS. Sponsored by DAPRA, "Project Maven" is an AI-based initiative that examines battle-prone area footage in an effort to eventually increase drone strike capacity there.

2.2 The Development and Categorization of LAWS:

Over time, LAWS have changed in tandem with AI. Gradually, the autonomous parts have grown to the point where humans are no longer involved in deciding whether or not to engage a target. The three groups into which LAWS have been divided or developed are indicated below. The one under debate is the completely autonomous one, in which using a weapon does not involve human intervention.



Semi-autonomous

"Human in the loop"

Weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator.

Includes "fire and forget" munitions

Human-supervised

"Human on the loop"

An autonomous weapon system that is designed to provide human operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur.

Fully Autonomous

"Human out of the loop"

A weapon system that, once activated, can select and engage targets without further intervention by a human operator.

2.3 AI's Role:

AI is now a highly competitive new technology. A second cold war would break out as AI became the focal point of the world power struggle. Today's truth is that AI is guiding us toward an algorithmic battlefield without borders where battles will be waged without the participation of humans. In the domains of internet and Geospace, this ecosystem will be hard to comprehend and manage. Deep learning and machine learning would make it easier to implement AI effectively. High-speed hardware with a huge memory capacity and new generation GPUs can handle big data analysis and very high-speed connection in addition to speeding up processing.

2.4 LAWS and UN:

In November 2019, efforts to control LAWs at the UN came to a deadlock once more. The UN had a discussion on the effects of LAWS on human rights. Governments called for the outright prohibition of AI-powered weaponry. However, the US and Russia both opposed the action and suggested that legally binding agreements be formed instead.

The CCW member nations were unable to agree on a resolution against LAWS during the conference. However, they have agreed to carry on with the negotiations to regulate deadly autonomous weapons systems during the following two years. UN envoys voiced dissatisfaction and accused Russia of diluting the agenda. Disappointed with the CCW's lack of advancement, NGOs have begun advocating against LAWS, calling for nations to negotiate as a separate treaty rather than through the UN convention.

UN Secretary-General Antonio Guterres once more urged the creation of a new international agreement that would outlaw LAWs during the just ended Paris Peace Forum. " Machines that are capable of killing without human involvement are politically and ethically abhorrent," he declared.

2.5 Cyber Security Challenges:

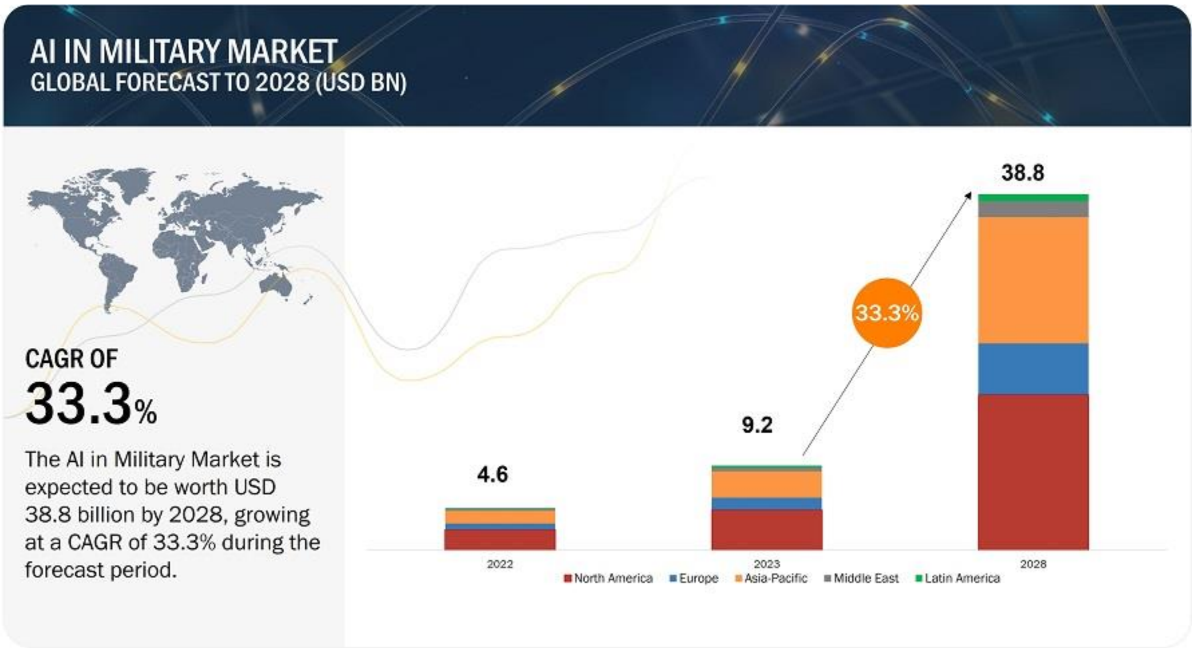
To ensure the safety of cyber-controlled weapons, there is an increasing need for a scalable, automated, high-speed vulnerability identification and patching system. An increasing number of military platforms are being linked together via internet backbone. Before being deployed, patches are made to prevent any hacking on embedded software-controlled equipment after an audit is conducted to identify any defective code or vulnerabilities.

The task of automating the process of finding vulnerabilities and concurrently repairing them in the cyber domain may be taken on by AI and machine learning. It can redefine the next phase of cyberwarfare by concurrently taking advantage of the weaknesses in hostile systems. We can boost the independence of interaction between physical and virtual environments in a variety of ways. Cyber operations can be employed in countermeasure operations as well as traditional weapon systems to boost autonomy. We have the ability to cause inadvertent interconnections and emergent behaviours amongst independent systems. Autonomous weapon systems will remain susceptible to cyber operations if they are not sufficiently firewalled.[1]

2.6 Growth:

The MAI market is projected to expand at a Compound Annual Growth Rate of 33.3% between 2023 and 2028, from its estimated US$ 9.2 billion in 2023 to US$ 38.8 billion by 2028. The development of highly precise military laser systems is a driving force behind the use of AI in the military industry.

[1] Lethal Autonomous Weapon Systems, *available at:* http://www.indiandefencereview.com/news/lethal-autonomous-weapon-systems-a-challenge-to-humanity/ (Last Visited on November 01, 2023).



3. INDIA'S POSITION ON AUTONOMOUS WEAPONS:

Over the past ten years, India has witnessed a renewed emphasis on matters related to national security and defense. In reaction to the 2016 terrorist assault in Pathankot, India carried out a "surgical strike" on Pakistani territory to demonstrate to the rest of the world that it would not hesitate to use force if necessary to defend itself against attacks like the one that occurred in Uri.[2] Similarly, the Indian Air Force retaliated to the Pulwama assault in 2019 with airstrikes deep within Pakistani territory in Balakot. That event resulted in the explosion of a convoy transporting paramilitary soldiers, killing at least forty people in Jammu and Kashmir.

The Indian government has now made it plain that it will not hesitate to cross border(s) or take action to disrupt operations against India, speaking with force through well-known speakers. Another example of foreign aggression in this case is the Chinese aggression that has elicited an equally forceful response from India is the Doklam impasse.[3]

But despite the focus on defense and national security, India's military spending is relatively small compared to countries like the US, China, and Russia. The Stockholm International Peace Research Institute claims that during the past 10 years, China's military spending has grown at the quickest rate. In China, it increased by over 83%, whereas in India, it increased by only 29%. While the US has cut its military spending by around 17% over the last ten years, it is still the world's greatest spender, paying more than twice as much as China.[4] As noted by the PSC on Defence (2017–18), Pakistan expended a higher proportion of its GDP (3.3%) than India did on defense.[5]

India is therefore trailing behind China, Russia, and the US in the race to develop LAWS and related technologies. India now allocates 2-2.5% of its GDP on defense.[6] It would be challenging to bridge the GDP gap with the aforementioned nations, even if it increased this amount to 3% as advised by the Standing Committee. It would be meaningless to just increase and redirect funding in an aimless manner toward the development and/or acquisition of LAWS.

India would benefit more by using its resources to create and apply LAWS in ways that are more appropriate for the nation. India simply cannot afford to commit its financial resources to an arms competition that is unlikely to end in its favour. Yet, by rationalizing and adapting LAWS development to its unique situation, it may make it more suitable for it.

3.1 LAWS: A Legal Remedy for India's Border Problems:

The Pathankot, Balakot, and Doklam episodes have not only changed India's national security strategy, but they also underscore a critical point: India's frontiers, where it is bordered by two countries that are essentially hostile, continue to be the country's greatest security threats.

India's frontiers are among the world's most heavily defended. India shares a total of 15,106.7 km of its international land border with China and Pakistan, 3,323 km of which are shared with the former. The 1,643-kilometer border between India and Myanmar and the 4,096.7-kilometer border between India and Bangladesh are two more noteworthy land borders. India deploys the biggest BSF in the world, with over 2.5 million troops, to defend these borders.

Nevertheless, there are drawbacks to using a large labour force to patrol vast distances. Their salaries and benefits, which already take up a sizable portion of the defense budget, must be paid. In the Union Budget for 2020–21, salary expenditures made up a whopping 30% of the defense budget; pensions accounted for the remaining 28.4%.[7] On the other hand, just 23% of capital outlays are related to building roads and bridges in border areas, as well as buying military hardware, weapons, planes, and naval vessels. The burden that revenue expenses like wages and pensions are placing on the defense budget is evident, and as a result, capital expenditures like acquisition and modernization wind up receiving less attention.

[2] The Inside Story of India's 2016 'Surgical Strikes', *available at:* https://thediplomat.com/2017/09/the-inside-story-of-indias-2016-surgical-strikes/ (Last Visited on November 01, 2023).

[3] India's armed forces now do not hesitate to cross border to protect country: Rajnath, *available at:* https://www.theweek.in/news/india/2020/02/26/India-forces-now-do-not-hesitate-to-cross-border-to-protect-country-Rajnath.html (Last Visited on November 01, 2023).

[4] Global Military Expenditures Are Up, Driven by Top 2 Spenders — U.S. And China, *available at:* https://www.npr.org/2019/04/29/718144787/global-military-expenditures-up-driven-by-top-two-spenders-u-s-and-china (Last Visited on November 01, 2023).

[5] *Ibid.*

[6] Demand for Grants 2020-21 Analysis : Defence, *available at:* https://prsindia.org/budgets/parliament/demand-for-grants-2020-21-analysis-defence (Last Visited on November 01, 2023).

[7] *Ibid.*

This is partly due to India's over reliance on labour. Right now, the largest ground force in the world is part of the Indian army. China, which has the greatest army until recently, has allegedly reduced its ground forces in half as a result of a significant modernization drive that began in 2015.

This is where India may benefit from autonomous weapons' force-multiplier effect. They can readily support border patrol units in detection and monitoring, such the BSF. Bigger aircraft can follow terrorists and their movements, such as the MQ-1B Predator. The RQ-11 Raven is a tiny, manually launched drone that was first created for the US military. It can provide soldiers on patrol with surveillance anytime it's required. It would also be very helpful to deploy a number of "South Korea's SGR-A1 Sentry Guard Robots" to monitor lengthy and hazardous borders, like the one between India and Pakistan. Israel has started using armed ground robots to guard its border with Gaza. These robots can also be configured to always keep people informed, which eliminates the chance of their going awry.

There's already some progress in this direction. If not outright autonomy, India is already concentrating on raising automation. According to reports, the Comprehensive Integrated Border Management System is equipped with several cutting-edge surveillance technology, including: *"thermal imagers, infrared and laser-based intruder alarms, aerostats for aerial surveillance, unattended ground sensors that can assist in detecting intrusion bids, radars, sonar systems to secure riverine borders, fiber-optic sensors, and a command-and-control system that will receive data from all surveillance devices in real time".*[8]

It is believed that two pilot projects in Jammu, Bangladesh, and along the border between India and Pakistan have been operationalized. To be clear, the BSF is modernizing its equipment to augment its border monitoring capabilities, and the CIBMS is a part of that effort. It should not be confused with autonomous weapons like the SGR-A1 from South Korea, which is still a long way off from the CIBMS. The BSF troops would receive information from the CIBMS continually and use it to dispatch QRTs to neutralize any threats. Drones and other unmanned aerial vehicles will be considered, even though the CIBMS primarily uses detection and surveillance tools like sensors and satellite imagery.

A thorough deployment of the CIBMS that utilizes both autonomous and automated technologies will greatly minimize India's border challenges. Naturally, AI and other technical advancements can only be employed as a force multiplier and cannot totally replace the foot soldier given the current state of technology. Still, it would greatly alleviate India's financial woes and problems with its human resources. The working conditions for BSF personnel are harsh. The "Department-Related Parliamentary Standing Committee on Home Affairs" has also noted and expressed concern about the fact that BSF jawans are sometimes refused basic facilities because of a system that keeps them from obtaining enough sleep because of a staffing deficit. As a result, the BSF recruits more personnel and increases salaries and pensions, which lowers the military budget's income to capital ratio and postpones modernization efforts. Technology can somewhat counteract this.[9]

India will similarly take a cautious approach to the creation and use of LAWS in accordance with its own unique criteria when it comes to its civilian AI policy.

In this context, the NITI Aayog has lately advocated in favour of an inclusive, long-term, and specially designed AI strategy for India. The "National Strategy for Artificial Intelligence #AIFORALL" discussion paper identifies the following topics as top priorities for AI development in India including healthcare, agriculture, education, infrastructure and smart cities, and intelligent mobility and transit. However, it only focuses on civilian applications of AI. "AI for the Greater Good," the text's guiding concept, ensures inclusive advancement for society as a whole. This is noteworthy in light of India's growing social inequities and digital inequality.

4. SHOULD IT BE BANNED:

The use of lethal autonomous weapons carries several serious concerns. Even for the most cutting-edge military projects in the world, these hazards vastly exceed any potential advantages. "The Third Revolution in Warfare" is the moniker given to these weapons because of their enormous potential to harm our society.

What are the primary dangers associated with the creation of this new kind of weaponry, and should it be banned?

4.1 Unpredictability:

The behaviour of lethal autonomous weapons is wildly unpredictable. Anticipating the activities of these weapons in real-world scenarios is a challenging task because to the intricate interplay between dynamic operating contexts and machine learning-based algorithms. Furthermore, in order to stay one step ahead of the opposition, the weapon systems are designed to act in an unpredictable manner.

4.2 Proliferation:

As they don't need expensive or difficult-to-find basic components, slaughterbots are incredibly affordable to make in large quantities. They are also difficult to find and safe to carry. Such weaponry is certain to spread once major military nations start producing them. They will soon be seen on the illicit market, where they will end up in the hands of warlords looking to carry out ethnic cleansing, tyrants seeking to subjugate their people, and terrorists hoping to topple whole countries.

4.3 Mass Destruction:

The scalability of lethal autonomous weaponry is quite high. This implies that your ability to cause damage with autonomous weapons is entirely dependent on how many Slaughterbots you have in your arsenal not on how many humans are available to use them. Unlike conventional weaponry, this is in sharp contrast: it is impossible for a military force to do twice as much harm with just twice as many weapons; in addition, it must enlist twice as many men to man those weapons. Any size swarm of Slaughterbots just needs one person to set it off, and each Slaughterbot in the swarm will thereafter fire on its own.

The combination of the significant risk of proliferation and the potential to scale up creates the possibility of widespread destruction. A weapon of mass destruction is defined by its ability to be used by one person to directly cause the deaths of several people. In the case of deadly autonomous weapons, a single person might potentially trigger a swarm of hundreds or even thousands of Slaughterbots. Scalability gives that person more power, and proliferation raises the possibility that vast numbers of these weapons will fall into the hands of someone ready to cause mayhem. Various autonomous weaponry systems, such as Slaughterbots are considered to be weapons of mass destruction.

4.4 Lacks Accountability:

Given the unpredictable nature of autonomous weapons, it raises basic concerns about who is ultimately accountable and liable for the use of force when algorithms are allowed to decide whether to use fatal force. Given that international humanitarian law mandates that those guilty

[8] Union Home Minister launches Smart Fencing on Indo-Bangladesh border, an effective deterrence against illegal infiltration, *available at:* https://pib.gov.in/Pressreleaseshare.aspx?PRID=1567516 (Last Visited on November 02, 2023).

[9] Parliamet of India, 203rd Report on Border Security: Capacity Building and Institutions, April 2017/Chaitra, 1939 (Saka).

of war crimes and serious violations of the Geneva Conventions be held legally accountable, one may argue that the "accountability gap" is unlawful. If military operators or commanders purposefully broke the law while operating a fully autonomous weapon, they may be held legally accountable. Legally and morally, it would be difficult to hold an operator accountable for an autonomous robot's aberrant behaviour.

4.5 Cyber Security Risks:

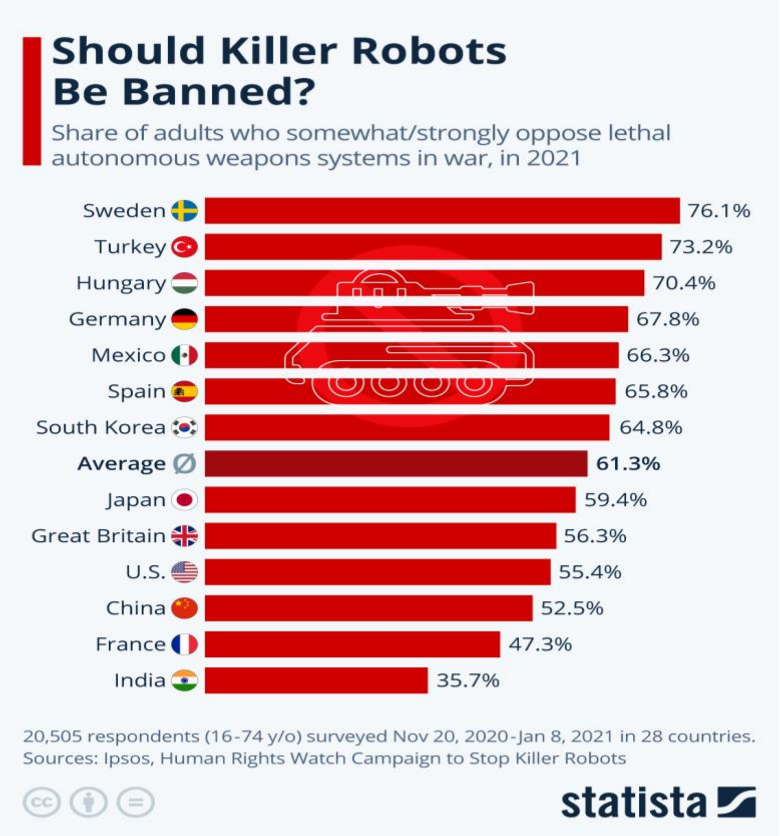
AI systems employed in combat are susceptible to cyberattacks, which may result in illegal access to, manipulation of, or control of vital military infrastructure. These weaknesses might lead to sabotage, undermine operational capabilities, or reveal confidential information.

4.6 Bias and Discrimination:

In training data, human biases can be inherited and amplified by AI systems, producing discriminating results. Biased AI decision-making in a military setting may lead to unjust targeting, innocent fatalities, or worsening of already-existing conflicts.

Ipsos Study:

According to study by Ipsos and the Campaign to Stop Killer Robots, the great majority of people on the planet still have negative opinions of deadly autonomous weapons systems in conflict. All but one of the 28 nations that were polled between November 20, 2020, and January 8, 2021, were primarily opposed to its usage. The below mentioned graph shows the share of adults who somewhat oppose lethal autonomous weapons. Hungary (70 percent), Turkey (73 percent), and Sweden (76 percent) demonstrated the most resistance to the deadly cars in 2021. With 56% of those questioned saying they either somewhat or strongly supported the use of the weapons, India, on the other hand, had by far the greatest level of support.



5. CONCLUSION:

Billions of dollars are being invested in AI research by nations such as the US, Israel, China, Russia, and the US. AI has the capacity to revolutionize the military's battle readiness. Nations can always gain a military advantage over rivals under AI leadership. India plans to improve its AI-based weaponry in the face of calls for the prohibition of LAWS. The newly established 17-member AI task group under the Ministry of Defence, which is composed of military personnel, contractors, and researchers, has recommended that India advance AI to improve armed force operational preparedness. To begin with, the task group has selected a small number of application cases, including as unmanned aerial vehicles, underwater boats, robotic weapons, and tanks.

Given the present rate of AI integration into military systems, it won't be long until war machines become susceptible to attack and lose human control. The UN and human rights organizations are fully aware of the threat and are working to avert this catastrophe. If AI is incorporated into Weapons of Mass Destruction (WMD), nations will enter a state of self-destruction. When activated, LAWS are hazardous systems that, in the absence of human involvement, would initiate counter and counter operations. In summary, we shall live in a world where deadly robots will battle it out for the benefit of their individual masters, who will seldom be able to control them. To save mankind, the UN must immediately oversee and regulate the development of LAWS, and India must play a bigger part in ensuring LAWS is safe.

REFERENCES

Book:

- Pravin Sawhney, The Last War: How AI Will Shape India’s Final Showdown with China (Aleph Book Company, 2022)
- Rajiv Malhotra, AI & The Future of Power (Rupa Publications, 2020)

Report:

- Parliamet of India, 203rd Report on Border Security: Capacity Building and Institutions, April 2017/Chaitra, 1939 (Saka).

Website Links:

- http://www.indiandefencereview.com/news/lethal-autonomous-weapon-systems-a-challenge-to-humanity/
- https://www.orfonline.org/wp-content/uploads/2016/05/ORF_Issue_Brief_143_Mohanty.pdf
- https://www.thequint.com/opinion/india-must-take-a-practical-approach-amid-politics-around-killer-robots
- https://iigsa.org/modern-warfare-and-autonomous-weapons-destructive-ways-of-alternative-technologies-in-india/
- https://www.ijlt.in/journal/killer-robots-or-soldiers-of-the-future%3A-legal-issues-and-india%E2%80%99s-role-in-the-lethal-autonomous-weapons-debate
- https://chanakyaforum.com/artificial-intelligence-in-military-systems-india-needs-to-bridge-the-technological-asymmetry/