JSS Law College
Autonomous
Kuvempunagar, Mysuru

JSS Journal for Legal Studies and Research [ISSN 2321-4171]

Analyzing the compatibility of Autonomous Weapon Systems (AWS) with existing IHL, principles, particularly the requirements for distinction and proportionality.

Najma Noushad [1]

ABSTRACT

The development of Autonomous Weapon Systems (AWS) creates many challenges for the application and interpretation of International Humanitarian Law (IHL). AWS, which exist in a wide range of human intervention, raise questions about the capacity of the weapon to implement the principle of distinction and proportionality. Distinction demands distinguishing between combatants and non combatants whereas proportionality prescribes that any civilian casualty must not be disproportionate with regard to expected military advantage. This analysis reaches into whether AWS, especially advanced artificial intelligence, can make such judgments reliably in dynamic and unpredictable conflict scenarios. The very concern are the ethical and legality of delegating life-and-death decisions to machines and the accountability gaps in the chain of command. Proponents argue that AWS can minimize human error and enhance compliance with IHL, but critics highlight the limitations of current technology in comprehending complex contextual factors.

The study concludes that without proper mechanisms for compliance with IHL, the deployment of AWS could undermine the humanitarian objectives of the law. To address these challenges, there is an urgent need for international regulation and technological safeguards to ensure AWS operate within the boundaries of ethical warfare.

Keywords: *autonomous, weapon, humanitarian, distinction, proportionality, combatants, non combatants*

For Citation:

Najma Noushad, 'Analyzing the compatibility of Autonomous Weapon Systems (AWS) with existing IHL, principles, particularly the requirements for distinction and proportionality.', (2025) Special Issue, JSS Journal for Legal Studies and Research, Pg No 56-70, <JSSJLSR Archive – JSS Law College>

1 The author is a student of Second Year LLM at the Department of Law, Central University of Kerala. E-mail: najmanoushadoo@gmail.com .

INTRODUCTION

The history of war has been characterized by various technological innovations and ideas, each considered to be more accurate, efficient, and strategically useful. AWS are the most recent and transformative among these, which operate with variable degrees of human oversight and can autonomously select and engage targets. There arise questions about their ethical, legal, and operational implications because AI systems are a sign toward automation for combat. The frequency with which AWS technology is becoming used, it raises strong necessities to implement their evaluation for compliance with (International Humanitarian Law)IHL. IHL referred to as the law of armed conflict, seeks to mitigate the impact of war on the individual and the conduct of hostilities under a rules of ethical conduct. Two underlying principles in IHL are the principles of distinction and proportionality. Distinction requires the differentiation of combatants from civilians and military objects from civilian objects to avoid harm to non-combatants. Proportionality dictates that such incidental loss of civilian life and damage to civilian objects incurs no disproportionate advantage anticipated from an attack. The principles-considered-with-human-decision-making, however-have unique hurdles in the context of applying them to AWS, without the moral and contextual reasoning inherent to human judgment. An argument in favour of AWS states that this technology does not have human emotions or fatigue, so the errors and conformance to IHL could decrease. Critics argue that current AI technology cannot understand complex scenarios while making subtle ethical decisions. Accountability is also a concern-once AWS acts lawfully, no one knows who is responsible: the operator, programmer, or commanding officer. It further raises deep questions regarding the human element in war, where reliance on AWS in military operations is becoming more significant. Traditional armed conflict is always conducted by human soldiers who bring contextual judgment, ethical reasoning, and emotional considerations to the decision-making process. AWS lack such intrinsic human qualities; instead, they depend on pre-programmed algorithms and machine learning models to analyze and act in dynamic combat environments. This reliance on automation challenges the applicability of IHL and risks eroding the moral accountability that has guided warfare

throughout history. Direct human involvement in decisions regarding who to target is lost with the absence of such participation, and thus there is a risk of dehumanizing war, as machines decide on life and death. Moreover, as AWS take more autonomy, existing legal frameworks fail to address issues that are critical, such as attribution of responsibility and compliance with humanitarian norms.

Definition of AWS

Autonomous weapons or better called Autonomous weapon systems – define modern warfare's future approach; it makes use of Artificial Intelligence and advanced robotic functionality. These weapons are mainly involved with identifying, selecting and hitting the targets without relying upon human input. Autonomous systems of weapons differ from regular semi-automated types in that they are supposed to work with minimal intervention, or none at all from humans. As their use becomes commonplace, it is essential to learn about their definitions, levels of autonomy, and key characteristics to effectively assess their role and impact in warfare. AWS are generally defined through their autonomy in performing core tasks, particularly targeting and engagement. According to the ICRC, AWS are weapon systems with autonomy in their critical functions, defined as the ability to select and attack targets without human intervention. AWS are distinguished from automated systems by the latter's rigid manner of performing pre-programmed tasks in a static way and also differ from remotely operated systems in that they need human intervention all the time. Autonomous weapons systems is also known as killer robots, they are weapons systems that use artificial intelligence (AI) to identify and kill human target without the intervention of human[2]. AWS employs sensors, data processing, and artificial intelligence to monitor and make decisions even when humans are not on site, in real-time.

AWS autonomy falls into three general categories. The first of these categories is "human-in-the-loop" systems where the human operator stays engaged directly with critical decisions like the choice and validation of a target. For instance, the category includes many of today's drones, where operators make control over strikes based on system recommendations. In this model, there is a reduction in the risk of unintended consequences because human judgment

2 Autonomous weapons, https://autonomousweapons.org 31 Nov 2024, 09.30pm

becomes central to lethal decisions. The second category of such systems is "human-on-the-loop" systems where the system operates autonomously, and it is monitored by a human who can intervene as appropriate. Air defense systems like Israel's Iron Dome exemplify this level of autonomy, automatically intercepting threats while allowing humans to override decisions if needed. The most contentious category, however, is "human-out-of-the-loop" systems, which operate entirely independently during critical phases. Hypothetical examples include autonomous swarms of drones capable of identifying and neutralizing targets without human input. These systems raise significant ethical and legal concerns, as they lack direct human oversight. These autonomous systems on AWS need multiple high technologies. Sensors become the central hub; these give the perception to these machines of what their surroundings look like, how the surroundings function, and allow for the perception of gathering of data on the environment. It encompasses visual cameras, radar systems, infrared sensors, and even acoustic detectors working together. In illustration, such sensors as thermal imaging fit can identify targets even under such lessor conditions as night time activities, adverse weather. Nevertheless, their reliability in more demanding clutter environments like in complex scenarios would thus expose them to some incorrect target identification.

Artificial intelligence and machine learning forms AWS's core functionality. These systems are programmed to analyze large amounts of sensor data, find patterns, and make decisions based on pre-determined criteria. For example, image recognition algorithms may enable AWS to distinguish between military vehicles and civilian ones. But these capabilities have their limits. AI systems rely on the quality and diversity of their training data. Biases in this data can lead to discriminatory or incorrect targeting, raising ethical and operational concerns. The communication and networking systems are another significant feature of AWS. These provide for the exchange of information with human operators or any other systems, ensuring coordination and flexibility. For instance, swarm drones communicate with each other in order to carry out synchronized attacks or gather intelligence. But this reliance on networks is also a weakness where AWS can be vulnerable to cyberattacks that may disintegrate their operations or result in unintended consequences.

AWS are designed for all manner of operational tasks, hence these are very versatile tools in modern warfare. Some of the common primary functions of AWS are the identification and engagement of targets. They are able to autonomously identify and prioritize targets by applying AI and sensors on finding armoured vehicles on a battlefield. They also have very common applications in surveillance and reconnaissance; they monitor enemy movements or gather intelligence in risky areas with much less danger to human personnel. Defensive applications are also prevalent, with systems like automated sentry guns protecting military installations by detecting and neutralizing potential threats. Additionally, AWS are increasingly being designed for swarm coordination, where multiple units operate collectively to overwhelm adversaries. While these capabilities offer tactical advantages, they also pose significant challenges, particularly in distinguishing between combatants and civilians or responding to rapidly changing battlefield dynamics. It thus gives an impression that there exists diverse fields where AWS are set across with complete deployment. In aerial combat missions, UAVs with either lethal or non-lethal loads dominate the landscape mainly targeting hits or surveillance. There exists support in combat or a defense role in ground base as AWS. In a maritime setup, autonomous submarines or even surface vessels are there and are used for both mine detection and reconnaissance along with offensive roles. Moreover, AWS are increasingly integrated into cyber warfare, with AI-driven systems to identify and neutralize digital threats and also autonomous weapon usually acts as a force multiplier.[3]

Even though AWS have developed their advanced capabilities, the defining characteristics of AWS introduce serious ethical and legal dilemmas. The delegation of decision-making to machines raises questions about the removal of human judgment from life-and-death decisions. This shift challenges traditional ideas about accountability, as it's unclear who is responsible—operator, programmer, military commander—for the actions of the AWS. Moreover, the possibilities for malfunction or unintended activity of the AWS could put civilian populations at risk of mass harm and violate the international norms of International Humanitarian Law.

3 Army University Press , https://www.armyupress.army.mil, Pros and Cons of Autonomous Weapons Systems, 31Nov 2024, 11pm.

International Humanitarian Law: Core Principles

International Humanitarian Law, also known as the law of armed conflict, is a set of rules designed to mitigate the human suffering caused by war. It aims at regulating the conduct of hostilities, protecting those who are not or no longer participating in combat, and limiting the means and methods of warfare. Rooted in international treaties like the Geneva Conventions and their Additional Protocols, IHL is a balance of military necessity with humanitarian considerations. At its core, IHL is guided by a few fundamental principles that underpin its framework: distinction, proportionality, necessity, and humanity.

1. The Principle of Distinction

This principle of IHL is one of differentiation between combatants and civilians as well as military and civilian objects.

Combatants and Civilians: Combatants are lawful participants in hostilities. They are the only target of armed conflict. On the other hand, civilians are civilians and protected from direct attacks unless they take direct part in hostilities.

Military vs. Civilian Objects:_Military objects, like enemy forces or weapon storage facilities, are legitimate targets. Civilian objects, like homes, schools, and hospitals, are immune to attack unless they are used for military purposes. The principle of distinction limits damage to civilians and civilian infrastructure during hostilities. It binds belligerent parties to use methods and weapons that can distinguish between legitimate and illegitimate targets. The principle is also challenged by the emergence of Autonomous Weapon Systems (AWS) because it is uncertain whether such systems can reliably distinguish between combatants and civilians. In cases where AWS misidentify targets, there could be grave violations of this principle with massive civilian damage.

2. The Principle of Proportionality

The principle of proportionality also prohibits attacks where the incidental harm to civilians and civilian objects would be excessive in relation to the anticipated military advantage. This principle recognizes that harm to civilians may occur, but it seeks to ensure such harm is not disproportionate to a military goal. For instance, a military strike on a military base in an

urbanised area would be disproportionate if expected civilian casualties exceed the operational value of the target. The principle of proportionality is particularly relevant in the context of AWS. While AWS may enhance precision and reduce the risk of human error, their ability to weigh military advantage against potential civilian harm remains limited. Machine algorithms lack the nuanced ethical reasoning required for proportionality assessments, raising concerns about their compliance with this principle.

3. The Principle of Military Necessity

Military necessity allows the use of force that is required for a legitimate military objective and is not prohibited by IHL in other ways. It justifies actions that are crucial to weakening the enemy's military capacity, provided they comply with other IHL principles. For instance, destroying a bridge used exclusively for military logistics may be justified under military necessity, whereas targeting a civilian structure with no strategic value would not. AWS must operate within the bounds of military necessity, avoiding excessive use of force or unnecessary destruction. The automation of decisions regarding what constitutes a legitimate military objective requires stringent programming and oversight to prevent violations of this principle.

4. The Principle of Humanity

The principle of humanity seeks to alleviate suffering and prevent unnecessary harm during armed conflict. It prohibits methods and means of warfare that cause superfluous injury or unnecessary suffering. This principle underpins the prohibition of certain weapons, such as chemical and biological weapons, that cause indiscriminate harm. It also emphasizes the humane treatment of prisoners of war, the wounded, and civilians. AWS pose deep concerns in applying the principle of humanity, especially when addressing their capacity to evolve to demanding moral and ethical judgments. For example, a maximum damage system that has been designed as an autonomous would unintentionally cause more suffering that goes against the intent of the principle.

5. The Precautionary Principle

The precautionary principle requires parties to undertake any available steps to avoid or to minimize injury to civilians or civilian objects in military action. This is going about

checking the legality of the target, issue warnings where possible, and weapons that cause minimal collateral damage. For instance, if precision-guided munitions are used instead of indiscriminate artillery in urban settings, then this principle is upheld. AWS, by design, are meant to be more precise and cause less collateral damage. However, the reliability of these systems in complex and unpredictable environments is still questionable. Without strong safeguards, their deployment could actually undermine efforts to ensure precaution in military operations.

6. The Principle of Non-Discrimination

The principle of non-discrimination is that all parties affected by armed conflict should be treated equally, without adverse distinction based on race, religion, nationality, or other factors. It guarantees humanitarian assistance, medical care, and protection be afforded equally to all civilians and combatants hors de combat (out of the fight). AWS must be designed to embody this principle: it has to ensure that there is an absence of discrimination in making decisions and providing equal treatment during hostilities.

Compatibility of AWS with the Principle of Distinction

The principle of distinction is the fundamental aspect of International Humanitarian Law, which asks warring parties to distinguish between combatants and non-combatants and military objects from civilian objects. In return, it makes sure that civilians, civilian infrastructure, and other persons not participating in the fighting are protected against attack, unless and otherwise they take an active part in hostilities. When it comes to AWS, their compatibility with the principle of distinction would depend on whether they are able to clearly identify and engage legitimate military targets without causing harm to protected individuals and objects. The principle of distinction still underlie the law of conflict .[4]

Technological Capabilities and Limitations

AWSs are equipped with advanced sensors, AI, and data-processing capabilities, which enable them to process vast amounts of information in real-time. These technologies enable

4 Elliot Winter, https://academic.oup.com the Compatibility of Autonomous Weapons with the Principles of International Humanitarian Law, 1Dec 2024, 7.26pm.

AWS to be tasked according to predetermined parameters, such as heat signatures, movement patterns, or weapon identification. For instance, AWS can differentiate between a military vehicle and a civilian car using image recognition algorithms. Such capabilities offer the promise of precision and efficiency in possibly reducing the risk of misidentification in combat.

However, these technological advancements are not without limitations. AI systems rely heavily on training data and pre-programmed algorithms, which may not account for the complexities of real-world scenarios. For example, combatants in asymmetric warfare often blend into civilian populations by avoiding uniforms or using civilian vehicles. These factors make it difficult for AWS to accurately distinguish between combatants and non-combatants. Moreover, sensor errors or environmental factors—like low visibility, urban clutter, or interference from electronics—can also limit the system's ability to distinguish correctly. A major weakness of AWS is that they do not understand context or exercise human judgment. The identification of a military target often requires subtle assessment, such as intent or subtle behavioral cues. While human operators may identify a non-combatant carrying a weapon for self-protection, AWS may consider him a legitimate target based purely on the detection of a weapon. There is a lack of contextual awareness leading to violations of the principle of distinction and, therefore, civilians may be harmed unintentionally.

Ethical Considerations

The ethical considerations of using AWS in the context of the principle of distinction are tremendous. The delegation of life-and-death decisions to machines raises questions about the moral accountability of these systems. AWS lack the human qualities of empathy and ethical reasoning, which are essential for making morally sound decisions in complex combat environments. For example, a human soldier would hold back from attacking if there was doubt about the identity of the target, erring on the side of caution and protecting civilians. AWS, in contrast, operate based on pre-set criteria and algorithms, leaving no room for ethical discretion. This delegation of decision-making also complicates issues of accountability. If an AWS erroneously targets civilians, it becomes unclear who should be held responsible—the programmer, the operator, or the military commander. This diffusion of

accountability undermines the ethical underpinnings of the principle of distinction, making it difficult to ensure compliance with IHL.

Balancing Military Advantage with Civilian Harm

AWS systems are often touted as something that can enhance precision and reduce collateral damage in warfare. AWS, with the use of sophisticated AI and machine learning algorithms, can analyze massive data to identify potential targets and the possibility of achieving military objectives. The computational efficiency makes it possible for AWS to pick the most effective method to neutralize threats while at the same time minimizing harm. For instance, an autonomous drone could detect and destroy a specific enemy vehicle while avoiding hitting the surrounding civilian infrastructure. Although this is so, AWS face considerable difficulties in trying to strike a balance between military advantage and civilian harm. Assessments of proportionality demand judgments in contexts that cannot be derived from analysis of data. The example of determining whether the destruction of a military warehouse in a populated area is worth the risk of civilian casualties would be based on considerations of ethics, tactics, and humanitarian considerations. AWS, on the other hand, are guided by pre-programmed criteria and cannot make such assessments. Furthermore, AWS are only as good as the quality of their programming and the data they have been trained on. Algorithms that do not take into account diverse and unpredictable combat scenarios may miscalculate the potential harm to civilians, which may lead to disproportionate attacks. For instance, an AWS may underestimate the blast radius of a weapon or fail to consider the presence of civilians in adjacent buildings, leading to excessive collateral damage. International humanitarian law still applies in a war against a brutal terrorist organization engaged in acts of absolute evil.[5]

Challenges in Contextual Judgment

One of the main challenges that AWS face when trying to comply with the proportionality principle is their inability to interpret context. Human decision-makers rely on experience, ethical reasoning, and situational awareness to judge the proportionality of an attack. They may look at the urgency of the military objective, the potential for evacuation of civilians, or

5 Liron A. Libman, Balancing Military and Humanitarian Necessities, https://jstribune.com , 1Dec 2024, 09.30pm

alternative strategies that might achieve the same goal without causing such harm. On the other hand, AWS relies on algorithms that lack flexibility when they are put into dynamic and complex environments. For example, in a fast-changing battlefield environment, a human decision-maker may opt to delay an attack so that civilians can clear the area, with humanitarian considerations taking precedence over tactical gains. AWS will, on the other hand, carry out the attack based on predetermined instructions, without regard to the greater ethical considerations. This inflexibility raises a high degree of risk, especially in urban or densely populated environments where civilian casualties are more probable. The uncertainty of war is another issue. Assessments of proportionality often have to be done in real time with less than perfect or conflicting information. AWS can process information quickly, but they do not have the intuition or judgment that a human has for such situations. This may make it difficult for AWS to apply the proportionality principle, especially in high-stakes or ambiguous situations.

Accountability and Responsibility within AWS Operations

AWSs basically do their job by delegating critical target detection and engagement decisions to the machines. This technological advance definitely improves military efficiency but poses tough accountability and responsibility issues in conflict. In war, an essential component of fulfilling its mandate of IHL would be accountability. Who and what will be held accountable is very hard to figure with AWS, and liability cannot seem to get enforced.

Accountability in Decision-Making

In conventional warfare, humans-the soldiers, commanders, and military institutions-are held accountable for decisions made while fighting. If a soldier breaches IHL, his action can be blamed on negligence, misconduct, or even intent; there are clear avenues for recourse in the courts. AWS disrupt this model of accountability because it operates with tremendous autonomy; decisions are frequently executed by the AWSs without human input. When AWS misidentifies the target or causes disproportionate damage, who is to blame can not easily be identified. Is the fault of the programmer in the algorithm design? The one operating and deploying the system? Or perhaps the commander who authorised the usage? This diffusion of responsibility creates accountability gap where each party can lay down their responsibility

on the computer because they did not do it themselves. The opacity of AI decision-making processes, often referred to as the "black box" problem, further exacerbates this issue, as it can be challenging to trace the reasoning behind an AWS's actions. This lack of accountability has grave implications for IHL compliance. The lack of a clear chain of responsibility could allow violations to go unpunished, thus weakening the rule of law and the humanitarian principles. Further, the lack of mechanisms of accountability may encourage the wanton use of AWS since those using them may feel they have no liability for their actions.

Legal Gaps and Chain of Command Issues

The introduction of AWS exposes significant legal gaps in existing frameworks. Current international law does not explicitly address the unique challenges posed by autonomous systems, leaving ambiguity around the allocation of responsibility. For instance, while commanders are typically held accountable for the actions of their subordinates, it is unclear how this principle applies to autonomous systems that act independently of direct human orders. Moreover, the chain of command is disrupted by AWS. While decisions flow from higher-ranking officers to lower-ranking personnel in hierarchies, each link bearing some level of accountability. In this case, AWS operate out of the structure, making decisions based on pre-programmed algorithms rather than human orders. This brings up the question of whether AWS can be called "subordinates" in the conventional sense and whether commanders can reasonably be held accountable for their actions. The lack of legal clarity is problematic for enforcement. For example, if an AWS commits a war crime, it may be difficult to prosecute a programmer or operator under existing laws, as they might not have the intent or negligence required for their role in the system's development or deployment. This calls for urgent legal reforms that address the special accountability issues of AWS. As AWS are increasingly found in the world, international scrutiny of their development, deployment, and use in warfare has become one of the burning issues requiring regulatory frameworks. International law today is not comprehensive enough to give guidance on these

challenges posed by autonomous systems. Different proposals for regulation have surfaced from states, international organizations, and civil society groups.

State of International Law Today

Existing international law, including the Geneva Conventions and their Additional Protocols, provides a robust framework for regulation of armed conflict. To this end, such bodies of law lay down very important principles that include that of distinction, proportionality, and military necessity. Most of these principles were founded with human decision-makers in consideration and do not explicitly address many of the complications introduced by AWS. For instance, IHL requires accountability for violations, yet it does not provide mechanisms for attributing responsibility to autonomous systems. Similarly, while IHL prohibits indiscriminate attacks, it does not specify how this principle applies to AWS that may struggle with target identification. In the absence of explicit legal provisions, states must interpret and adapt existing laws to regulate AWS, leading to inconsistencies in their application. Some of them say that AWS does not need new laws provided it is implemented in conformity with the requirements of IHL. For others, though, unique problems in AWS like a lack of accountability and an ethical dilemma call for something that requires new regulations as such.

Regulation Proposals

There are many proposals geared toward solving the issues created around the regulation of AWS. Several initiatives have come into limelight based on the advocacy for pre-emptive bans of complete autonomous weapons by campaigns like “Stop Killer Robots”. Supporters, who believe in such action, point to these as posing risks unacceptable to people and human rights; they urge a ban on AWS as they become ubiquitous. The third one would be the establishment of an international treaty that would have legal enforcement powers over the development and utilization of AWS. This international treaty could provide provisions on requiring human control over critical decisions, mandates for transparency in AI algorithms, and mechanisms for accountability for violations. Some states and experts suggest a more cautious approach, where non-binding guidelines or codes of conduct could be the first step toward regulation. These frameworks would allow states to be flexible in their adaptation to

emerging technologies while encouraging adherence to humanitarian principles. Despite these efforts, progress on international regulation has been slow, with disagreements among states over the need for new laws, the definition of AWS, and the scope of potential restrictions. This lack of consensus underscores the importance of continued dialogue and collaboration to address the challenges posed by autonomous systems.

Recommendations and Future Directions

To ensure the responsible development and use of AWS, several key recommendations can be made. First, states should prioritize transparency in AWS design and deployment, requiring developers to provide comprehensive documentation of their systems' capabilities and limitations. This would increase accountability because responsibility for violations could be more clearly attributed. A "human-in-the-loop" approach should be made mandatory for critical decision-making processes, with humans holding final authority over the use of force. This would likely alleviate many of the ethical and legal concerns associated with fully autonomous systems. International cooperation is also necessary. States, international organizations, and civil society actors should cooperate in defining clear definitions and standards for AWS and in the creation of mechanisms for monitoring and enforcement. For example, the establishment of an international supervisory body to examine and endorse AWS with regard to their conformity to IHL may provide a much-needed oversight. Another important research direction is about the ethics of AWS. Policymakers and technologists should join forces to engineer systems not only compliant with IHL but also aligned to broader humanitarian values. Investments in AI should be made along lines such as ethical reasoning, contextual awareness, and robustness under complex combat situations. Finally, capacity-building efforts should also be made to ensure all states have the resources and capacity to regulate and oversee the AWS. This includes making the military personnel trained on ethical and legal implications of employing the autonomous systems and promoting awareness of the public and the relevant debate about the role that AWS will play in warfare. Lastly, international negotiations on the regulation of AWS should be resumed. These negotiations should aim to build consensus among states in relation to AWS regulation,

given that disagreements over scope and nature persist. Though not exhaustive, incremental progress is attainable through agreements over such items as transparency and accountability measures. We should prohibit unpredictable autonomous weapons.[6]

Conclusion

The emergence of Autonomous Weapon Systems heralds a paradigmatic shift in war conduct, an opportunity and a challenge at the same time. Although AWS promise enhanced precision, efficiency, and operational capabilities, concerns about their conformity with IHL arise based on such questions as accountability, responsibility, and the moral implications of giving up life-and-death decisions to machines. The existing principles of IHL, namely the principles of distinction and proportionality, offer a solid ground for governing the employment of AWS. These principles were built with the human decision maker in mind and cannot sufficiently accommodate the singular issues associated with the autonomous systems. There exist no suitable legal structures which can handle questions like the diffusion of responsibility and limitations that machine algorithms can bring forth in complicated dynamic battle settings. There are plans underway to control AWS; the proposals run the gamut from an absolute ban, the creation of binding legal instruments, to guidelines not obligatory to any signatory to an instrument. Progress is gradual but the problem at stake necessitates a continuous discussion internationally, with concerted action being pursued by all the state parties and interested parties in a commitment towards transparency, accountability, and ethical responsibility so as to ensure AWS can serve in humanitarian functions, coupled with IHL. In conclusion, AWS regulation is not a mere legal or technical challenge but rather a moral imperative. Warfare is evolving, and thus the frameworks that govern it need to evolve with it. This is how the use of emerging technologies will continue to be consistent with the basic principles of humanity, dignity, and justice. The future path lies in balancing innovation with responsibility, safeguarding both security and human rights in this era of rapid technological change.

6 Autonomous weapons, https://www.icrc.org , 3Dec 2024, 09.30pm