# Table of Contents

Summary .................................................................................................................................................. 3

What is AWS? ........................................................................................................................................... 4

Relevance .................................................................................................................................................. 5

Technical Background .......................................................................................................................... 7

Existing Law on LAWS ........................................................................................................................ 11

- Arms Control & Disarmament ......................................................................................................... 11

  - Convention on Certain Conventional Weapons ............................................................................. 11

- Laws of Armed Conflict ..................................................................................................................... 12

  - The Geneva Conventions and Additional Protocols ..................................................................... 13

- Customary Law: the Principles of Necessity and Proportionality ................................................... 13

  - Martens Clause ............................................................................................................................... 14

- Just War Theory ................................................................................................................................. 15

- Data Privacy Law ............................................................................................................................... 15

- Regional Protections .......................................................................................................................... 17

- UNOOSA Remote Sensing Principles ............................................................................................... 18

- Right to Privacy ................................................................................................................................. 18

- Product Liability Laws ....................................................................................................................... 19
Ethical Considerations ........................................................................................................ 21

   In Humanitarian Terms ................................................................................................ 21

   Laws of Conflict ........................................................................................................... 21

   Emotional Distance ...................................................................................................... 22

The Technical Perspective ............................................................................................... 23

   Civilian Data Usage .................................................................................................... 23

   Data Bias ..................................................................................................................... 24

   Battlefield Singularity ................................................................................................. 24

   Hijacking and Bad Actors ........................................................................................... 25

Legal Accountability: Gaps in the Law ........................................................................... 26

Recommendations ........................................................................................................... 26

   International Legal Governance .................................................................................. 26

   States and State Militia ............................................................................................... 27

   NGOs, Non-profits, and the Private Sector ................................................................ 27

Conclusion ..................................................................................................................... 28

Works Cited .................................................................................................................... 29
Summary

Can Autonomous Weapons Systems (AWS) be used ethically? I argue that AWS cannot be used ethically until significant oversights in law are addressed and reconciled with emerging technologies.

I will elaborate the ethical context of AWS in this paper. After setting the scope and definitions of the paper, I explain the pertinence of this discussion. Next, I endeavor to explain in layman’s terms some key technical features of AWS. From there, I examine existing international law on AWS, and the equally relevant international law on civilian data usage. This analysis leads into the ethical considerations of AWS. Finally, I make bullet point recommendations to state and private actors on how to integrate ethical insurances into AWS use. This paper is a non-technical primer of the technical aspects of AWS, and connects these actualities to ethics. I articulate the ethical context of AWS on four fronts: humanitarian, military, technical, and legal. My goal for these articulations is to highlight gaps in AWS oversight.

I would like to thank the OISTE Foundation for sponsoring and publishing this work; however, the views stated are my own.
What is AWS?

The word “autonomous” implies automation— the ability of a machine to reach an actionable decision independently of a human controller.¹ The human controller should have veto power over whether the machine-proposed action may execute or not; the machine is not fully independent. This veto power may or may not include manual correction, depending on the design of the machine in question. A weapons system is any machine intended as weaponry, whether defensive, offensive, or investigative. This variety includes anything from guns to missiles to submarines. Taken together, AWS is a weaponized machine that mechanically produces some potential action that a human controller must then authorize or cancel.

For the scope of this paper, I will discuss AWS that identifies striking targets using machine learning. This specific type of AWS is of ethical interest because of the margin of error introduced to the system by machine learning. Furthermore, its use draws in the ethical issues of data privacy. Some examples are Unmanned Aerial Vehicles (UAVs) capable of engaging targets independent of a remote human controller, or mine radars that can launch attacks against enemy submarines when they draw near. These technologies already exist.² This paper will refer to the specified range of weapons above as

---
² See the Harpy and MK 60 Captor Mine, respectively: https://www.iai.co.il/p/harpy; https://www.vp4association.com/aircraft-information-2/32-2/mk-60-captor-mine/
Lethal Autonomous Weapons Systems (LAWS), and abstract that group in their current incarnations and potential future forms. The term “lethal” specifies AWS that engage targets.

This paper is not about artificially intelligent weapons systems, which as yet do not exist in the true sense of intelligence. The particular ethical dilemmas posed by LAWS are unique from those of the artificially intelligent, which by definition would closely mirror human ethics. If a machine were fully capable of understanding the moral, psychological, and ethical aspects of war, the dilemmas posed in this paper would be moot. As yet, however, truly artificially intelligent machines do not exist. Only autonomous machinery does, which cannot grasp humanity. This paper is concerned with the particular lack of self-awareness LAWS operate by, and the issues this deficit raises.

Relevance

The United States Civil War is considered one of the bloodiest conflicts in that nation’s history. One of the main reasons the war was so devastating was because of the improvement in weapons technology.³ Guns had become more lethal in accuracy, range, and speed. This is just one anecdotal example of how improving weapons can come at a higher human cost. Conversely, weapons that can

improve accuracy to the point of surpassing human decision-making capacity would save lives. LAWS could take us in either direction, depending on human oversight.

Currently, there is not enough oversight of LAWS, and the conversation is starting late. Already, there are several LAWS that have been deployed in real combat. Some examples are Israel’s Harpy, an UAV that can target and engage enemy radars. Another is the infamous case of a drone acting on its own to fatally engage targets in Libya— the STM Kargu-2 drone.\(^4\) The American Long-Range Anti-Surface Cruise Missile scans, identifies, and engages naval targets.\(^5\) Similar and more advanced technology is certainly under development worldwide. The United States, Russia, the UK, and China have all voiced their intent to continue LAWS development.\(^6\) For nations seeking military advantage, their motivations are obvious. Other nations may be motivated to develop LAWS in order to remain on a level playing ground with the rest of the world. Proliferation has just begun.

This is not meant to be alarmist, however. Theoretically, LAWS have the potential to decrease harm in warfare. LAWS have the potential to ascertain and aim for targets more accurately than human combatants. They also reduce the number of human combatants required to be in combat range. Not only does this keep more humans out of danger, but it also reduces the logistical operations and cost


required to sustain human combatants on the move. Human combatants are historically and
notoriously poor at making objective decisions in combat—LAWS remove the risk of vengeful acts of
violence in war. LAWS can also maneuver where humans cannot—physically extreme terrains, for
example.

The potential for harm that LAWS pose is enough, however, to halt the discussion of pros.
LAWS are vulnerable to unanticipated harm—through poor programming or hackers—and to
committing violence at a previously unseen rate. Finally, a clear lack of legal oversight of LAWS must be
addressed before states can ethically pursue further LAWS development, if at all. This paper seeks to
identify these gaps in the technology and law comprehensively such that they be corrected. These gaps
are of international benefit to address given the potential for harm that terrorist actors could inflict
with the power of a hijacked LAWS. Despite major popular campaigns to stop the development of
LAWS, their proliferation continues. A synthesized consideration of the technology, laws, and ethics
that make up the discussion of LAWS is needed to advance the discussion from impasse.

**Technical Background**

What is the autonomous mechanism of LAWS? What renders the system capable of receiving
data, processing it, and producing a result? Any function inherently works on an input-output basis.
LAWS specifically process an input of data to produce a mechanical output. I will outline below some of the basic technological ideas animating LAWS and future LAWS.

A given LAWS may have multiple input channels. A LAWS might have a camera for collecting live visual data, or a geolocator function that tracks its position. Or it may have radars that pick up frequencies. The combinations of possible inputs are endless, and depend on the intent of a specific weapon. One example of a type of sensor system that can be used in LAWS is WAMI, or wide area motion imagery, a type of visual data collector that collects information from a large region of land. WAMI was developed by the United States and employed in real combat as early as 2006 in Afghanistan. It has since spread to other nations and been refined.7 Multiple data inputs can be processed in a sensor fusion system, a method in artificial intelligence employed to synthesize and render more accurately a machine’s perception of its environment.8

Once a central or graphics processing unit has processed the incoming data, machine learning can be used to “make sense” of the data. Not all LAWS use machine learning; however, the development of machine learning in LAWS is of concern to this paper. Machine learning is a system of algorithms that can organize data. One type, a convolutional neural network (CNN), can interpret

---


visual data to identify objects in a frame through layers of algorithms. Machine learning algorithms are characterized by data training— in other words, a human programmer feeds the software data sets to “train” the system to “recognize” objects. I put these anthropomorphic verbs in quotations to clarify that the system is not humanly intelligent, but responding to data with complex algorithmic structures that allow it to predict the likelihood of a new data set containing an object it has been trained to identify.9

The software can distinguish objects in a data set not because of true intelligence, but because of a neural network. True intelligence would imply that the software understands what the object it distinguishes is; i.e., it can understand a concept like “cat” if you give it visual data of animals. Understanding the concept of “cat” goes beyond the ability to recognize it, loosely like humans’ ability to recognize parts of speech in foreign languages without understanding what they are reading. A “cat” object to a computer might mean a particular set of data attributes are most of the time a cat in visual data sets. This sort of technology is relevant to LAWS specifically as they are already in use and under development. For example, a former branch of Samsung built and deployed an unknown number of autonomous sentry guns to man the Demilitarized Zone between the Koreas. The guns, using sensor

technology, could identify and distinguish between unauthorized or enemy humans in the zone versus animals, authorized humans, or natural disturbances.¹⁰

The neural network accomplishes visual identification by a series of connected algorithms. The algorithms, fed training data sets, can then produce a probability that a new data set contains certain objects it has “learned.” It is called a neural network because the system of algorithms loosely models human cognition processes in network form. Neural networks have been popularly called “black boxes” as the exact process of the algorithm system is not fully understood by humans yet. Neural networks can have multiple “layers” of algorithms, increasing their complexity. In its most fundamental form, a neural network only has an input and an output layer. Layers in between these are called hidden layers. Given enough data, time, and hardware, a neural network could identify objects to a high probability of likelihood. The catch is that no machine has infinite data, time, or unbiased programmers to train it to ideal accuracy and efficiency. Furthermore, no programmer yet fully understands this autonomous mechanism.

Existing Law on LAWS

Currently, there is no detailed, explicit, or comprehensive international law on LAWS. Relevant international law includes arms control, laws of armed conflict, data privacy law, and product liability law. Below, I will outline the pertinent scope of each. As they overlap, these laws parameterize what we can and cannot extrapolate from existing law on the legality of LAWS, and specifically, its use. No international law yet exists that defines LAWS and allows or disallows its manufacturing or use in combat.

Arms Control & Disarmament

Convention on Certain Conventional Weapons

In 1980, the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW) took place in Geneva with fifty original state signatories. The Convention has since been expanded and amended, today including a third annex adopted in 2019 by high contracting parties on the relevance of the CCW standards to LAWS. This annex is entitled “Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System.” The gist of the CCW is
outlined in the full title: to prohibit or restrict unnecessarily powerful weapons. This agreement is advantageous to signatories as it protects combatants and civilians alike, and promotes some measure of mutual trust and agreement on the conduct of warfare. The annex on LAWS, however, does not explicitly define LAWS or enforce oversight. The language characterizing LAWS in this annex is inclusive of future LAWS—i.e., “emerging technologies” but vague. The significant legal overtures proposed by the group in the annex are the following:

- a) An assertion that International Humanitarian Law applies to LAWS
- b) That legal accountability for LAWS falls on human operators and not the machines themselves in the spirit of non-anthropomorphism
- c) Caution in development and use should be practiced

Laws of Armed Conflict

The laws of armed conflict are the set of rules governing conflict under International Humanitarian Law (IHL), Customary Law, and various moral theories. I will discuss core IHL tenets, Customary Law, and the Just War Theory below as they are relevant to LAWS.

---

The Geneva Conventions and Additional Protocols

The Geneva Conventions are the core articulation of International Humanitarian Law and its aim. The four conventions and their protocols fundamentally encompass the following tenets: the humane treatment of the wounded and prisoners; the distinction between civilians and civilian objects from combatants; the disallowance of hostilities against civilians and civilian objects; what constitutes war crimes. The two Additional Protocols of 1977 further emphasize the duty to minimize damage. The first Additional Protocol of 1977 explicitly applies this obligation to the “means and methods” of warfare; that is, weaponry.\(^\text{12}\) Therefore, under the Geneva Conventions, LAWS must be able to distinguish legitimate targets and minimize harm.

Customary Law: the Principles of Necessity and Proportionality

The Principles of Necessity and Proportionality are contained in spirit in the Geneva Conventions, but trace their origins back further into customary law. Customary law are those moral rules that are generally accepted, and become so through practice over history. Written International Humanitarian Law simply articulates and supplements customary law,

\(^\text{12}\) Geneva Conventions and their Additional Protocols. 
encouraging compliance through international litigation. The Principle of Necessity\textsuperscript{13} is the rule of thumb that military actions are strictly necessary for military aims that are sound by the laws of armed conflict. The Principle of Proportionality\textsuperscript{14} states that military actions accomplish more than they harm civilians or civilian objects. Therefore, under these principles, LAWS must only execute necessary, legitimate military actions that do not excessively harm civilians.

\textbf{Martens Clause}

Within the Hague Conventions, fundamental international documents on the conduct of war, is the Martens Clause. The Martens Clause dictates that if a particular or more detailed code of law is not adopted or written, then the conduct of war in question is still subject to customary law, and “the laws of humanity and the requirements of the public conscience.”\textsuperscript{15} Therefore, LAWS must be subject to customary law until more detailed law is written. The last conditions of the Martens Clause—those on humanity and public conscience—are more subjective. Given the wide unpopularity of “killer robots,” should


LAWS be illegal on this condition? \textsuperscript{16} Many authoritative voices, including the Human Rights Watch Campaign, \textsuperscript{17} have spoken against the use of LAWS on the basis of International Humanitarian Law.

**Just War Theory**

Just War theory is the general theory of the humanitarian conduct of war. The laws already discussed above fall under it, as do some additional traditional principles established in the Western tradition. Of interest is the idea that war or actions in war have a “reasonable chance of success.” \textsuperscript{18} This is relevant to LAWS because it adds a moral requirement to the success rates of the technology in LAWS, which is not absolute.

**Data Privacy Law** \textsuperscript{19}

LAWS use data to execute their function. Information and location privacy therefore must be part of the conversation of the legality of LAWS. For example, LAWS that use facial recognition or similar software should be subject to the pertinent laws... but whose? In warfare, should a foreign

\textsuperscript{16}Stop Killer Robots. Campaign to Stop Killer Robots. https://www.stopkillerrobots.org/

\textsuperscript{17}See their unequivocal stance against LAWS here: https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots

\textsuperscript{18}Moseley, A. “Just War Theory.” Internet Encyclopedia of Philosophy. https://iep.utm.edu/justwar/

force’s LAWS be subject to data privacy law of the country in which they are using or designing the LAWS? How long should LAWS used in combat be allowed to store data? Besides biometric data, what about location data or other personal data types?

For LAWS that use machine learning, what laws apply to the data the software uses as training sets? Should this data be what is publicly available on a given population, say if the LAWS must be able to visually identify combatant uniforms? Or for accuracy’s sake, should the LAWS be able to sample data from live visual input, like WAMI? In order for a LAWS to abide by international humanitarian law and distinguish between civilians and combatants, it needs to be able to access civilian data. There are several disparate law systems on data privacy that may apply to LAWS, and some specifically in the context of data used in cyberwarfare. However, there is no substantial legal literature on the use of data in LAWS specifically.20

As the laws outlined below will illustrate, there is an indirect conflict of interest between data protection and privacy laws and the core of International Humanitarian Law. LAWS, by the laws of armed conflict, must be able to distinguish between civilians and combatants. Furthermore, LAWS must abide by the principle of proportionality. Must the use of private civilian data be proportional to the military target achieved? How can this proportionality be measured? Finally, given that the more

---

data that is accessible to LAWS makes LAWS systems like machine learning more accurate, should civilian privacy be given priority over the accuracy of LAWS? The more privacy protections given to civilian data, the less LAWS can leverage that use civilian data, thus reducing its capacity to distinguish. On the contrary, if a LAWS software has access to more data, its capacity for accurate targeting and execution decisions will increase. How much “situational awareness” should LAWS be granted, under data privacy laws given this trade-off?

**Regional Protections**

There are several regional data privacy laws that may be of relevance to this discussion. For example, the GDPR (General Data Protection Regulation) of the European Union protects private individuals’ data against all enterprises, domestic or foreign, that can process or store the data in question.\(^2\) Around 70% of nations worldwide have some legislation in place on data protection and privacy.\(^2\) However, there is no comprehensive body of law that details individuals’ rights on personal data during warfare. Again, these laws face a geographic dilemma: what set of laws should parties to combat follow if the conflict is cross-border?

---

\(^2\) General Data Protection Regulation. European Union. [https://gdpr-info.eu/](https://gdpr-info.eu/)

\(^2\) UNCTAD, “Data Protection and Privacy Legislation Worldwide.”
UNOOSA Remote Sensing Principles

Satellite imagery has long been used in intelligence agencies worldwide. This type of data is a sure and open source of intelligence to determine large physical movements on Earth–ships, facilities, and gatherings of various types. Given the abundance of satellite imagery available, state and private actors generally cooperate on the openness of this source of intelligence. Satellite technology that can distinguish individuals’ faces is not yet in use, despite a concerning deficit of international regulation. Some states actively prohibit their own technology from taking such high-resolution images, but not all do.23 The largest international body of law on satellite imagery to date is the UNOOSA's Remote Sensing Principles.24 However, this document does not explicitly address privacy concerns, and only stipulates that satellite activity adheres to “norms” of international law.

Right to Privacy

Under the Declaration of Human Rights, Article 12 articulates the right to privacy:

---

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.\textsuperscript{25}

This statement could be applicable to the legality of LAWS that use private individuals’ data. For example, LAWS that visually scan building types in order to select and target buildings with characteristic features of their combatants must scan civilian buildings in order to make a distinction. Should these LAWS be allowed to thus observe homes? Should these LAWS be able to store these data for further reference and to refine its capacity to distinguish?

\textit{Product Liability Laws}

LAWS designed and manufactured within a certain state may be subject to the laws of product liability of that state. It is generally agreed that should a LAWS malfunction, the state that authorized its use in combat is liable.\textsuperscript{26} LAWS should therefore be subject to their state of origin’s liability laws. However, these generally domestic laws may come into conflict with the international obligation to distinguish between civilians and combatants. There is an error in machine learning, which some LAWS may employ for targeting functions, called overfitting.


Overfitting occurs when a software is trained on certain datasets repeatedly or of homogenous content. The software, when given a new data set, will then make obvious errors because of the biased data. For example, a software trained to distinguish between the binary genders, trained on data sets containing images of middle-aged adult faces, may completely fail when given an image of a young adult or a very old adult. These errors are the result of programmer bias. It is up to the programmers to decide what data on which their software is trained.

In the context of warfare, this tendency to bias becomes even more dangerous given high stakes and cultural ignorance. For example, a programmer from one culture may not fully understand the nuances in dress of another culture, and thus provide poor data to their software that must be able to distinguish between civilians and combatants. Given a LAWS that employs machine learning that has an overfitting error which is only discovered in real combat, who would be responsible for this machine? The manufacturer that produced it, under product liability laws? Or the state that authorized the deployment? How can manufacturers and states ensure that their LAWS do not fail to abide by IHL in combat? If a given LAWS cannot be proven reliable, it should not be deployed.

However, it is difficult to decide what level of reliability should be proven before a LAWS can be authorized for deployment. Human combatants must make split-second

---

decisions in close combat. Yet, civilian casualties still occur by accident. It is difficult to calculate the rate at which civilian casualty by accident occurs. Human combatants are also highly prone to irrational decision-making in combat: that is, killing civilians out of rage, distress, revenge, hatred, etc. Any LAWS, even with the most rigorous training, will still make mistakes. At what threshold of mistakes is a LAWS more reliable than a human combatant? And what if programmers transfer their emotional biases on a given war into the machinery?

Ethical Considerations

Below, I will reiterate and synthesize ethical concerns on LAWS, drawing together technical aspects of LAWS. I will show why LAWS cannot be used ethically given their legal context.

In Humanitarian Terms

Laws of Conflict

LAWS may be inherently incompatible with International Humanitarian Law and its underlying principles. There is no technologically possible way to produce a LAWS and guarantee it will not commit errors. Given the highly impressionable nature of machine
learning, prone to programmer bias and thus poor accuracy, LAWS producers cannot guarantee they will work with the degree of success stipulated by the Martens Clause. Furthermore, LAWS cannot distinguish between civilians and combatants with full precision. Until we can fully understand the “black box” of neural networks, we cannot explain or address the flaws in LAWS systems. It is therefore unethical to deploy such weapons as we cannot completely control them. While the point of LAWS is to relinquish some human control, we cannot in good conscience do so until we can guarantee they will outperform human combatants in objectivity and humanity.

**Emotional Distance**

Perhaps the strongest argument for LAWS is also its weakest: while LAWS remove the dangerous human combatant from battle, LAWS likewise remove the compassionate human combatant. LAWS, under perfect technical performance, would not act violently out of revenge, hatred, or fear as a human combatant might. However, LAWS cannot grasp the moral contexts of combat, and thus cannot show mercy nor gain cultural understanding in a moment of moral choice. While LAWS keep humans safe by removing them from the battlefield in the case of remotely-operated LAWS, they also increase the emotional distance of combatants from the battlefield. War is destructive, and part of the cost of that destruction is the toll of
witnessing it. The human urgency we feel to end wars when we see destruction may fade if human combatants take a less active role in war.

The Technical Perspective

Civilian Data Usage

It is doubtful whether LAWS with machine learning can respect individual privacy in warfare. As discussed earlier in this paper, LAWS with machine learning are more accurate when they have access to more data. In order to better respect the necessity of distinguishing civilians in combat, LAWS must use more data. However, these data may be private or should be private. Can a balance be struck between maintaining data privacy and improving LAWS technically? Do private citizens’ privacy rights matter less during warfare? What data LAWS may access about civilians’ locations, homes, appearance, and habits must be regulated, as well as how LAWS procure and store that data? Given the lack of international discussion on civilian privacy during warfare, LAWS cannot yet be in the ethical clear. Furthermore, this discussion must involve civilians as they are a directly affected group. Their opinion on whether LAWS should be allowed to video them, sample their location data, identify them, or categorize them for the sake of warfare is vital.
Data Bias

As already discussed, LAWS are highly prone to error. Besides hardware malfunctions, machine learning software is prone to echo human bias. LAWS, machines intended to perpetrate harm, cannot ethically afford to make mistakes. The stakes are life and death. If a LAWS incorrectly identifies a target, a human controller must override it. LAWS must therefore always be less than autonomous: they can only preserve ethics if they are automated but not independent. Furthermore, the responsibility falls on human programmers to provide sufficient, unbiased data training to machines. Programmers, ethicists, and military experts must therefore all be involved in the design process as programmers cannot be expected to anticipate the nuances of warfare or warfare ethics.

Battlefield Singularity

“Battlefield singularity”\(^28\) is the term for warfare at a speed too fast for humans to process, such that humans review the results after the conflict has been fought. It is unethical to place human combatants on this kind of battlefield, knowing they will be killed quicker than they can defend themselves. Perhaps this sounds like science fiction, but it is currently on the radar of Chinese military tech development. Concerning developments like these fuel the arms

race to maintain equal force among military powers, increasing the potency of LAWS. Furthermore, at high speeds, humans cannot stop an assault if they cannot process it.

**Hijacking and Bad Actors**

LAWS are prone to hijacking in physical and cyber space. LAWS hardware necessarily exists in physical space that must therefore be guarded against human-access hacking. LAWS software must be similarly guarded against cyber attacks. Personnel operating the LAWS must be trained in cybersecurity and understand the security risks posed by cyber warfare and keeping LAWS details confidential. Any internet or communications systems LAWS access must be secure, especially remotely-operated LAWS. LAWS, if hacked, pose a serious threat to all human life. Lone hackers, terrorist and criminal groups could perpetrate immense harm given access to LAWS. Bad actors in the design process could also compromise LAWS integrity by purposefully biasing machine learning data, or compromising human control checks in the LAWS function. Domestically, states could severely damage human rights by using LAWS on their own citizens, for example at border control or as a policing system. The potential for wrong is immense. The use of LAWS opens up new fields of cyberwarfare as actors battle for control over LAWS more powerful than their own. Given the development of borderless and private hacker collectives, and competition among state militias, the threat of hijacking should act as a main incentive for reluctant states to participate in international regulation of LAWS.
Legal Accountability: Gaps in the Law

There is not enough legislation specific to LAWS. Currently, international laws that apply to laws only do so peripherally as explored above. International regulation of LAWS is essential to ensure safety, ethics, and non-proliferation in an emerging and dangerous arms race. The technology behind LAWS is simply insufficiently understood and regulated to be deployed in combat with humanitarian confidence. Until regional and international agreements on LAWS are decided, which regulations on data, liability, and use of force apply to a given LAWS is ambiguous. This ambiguity extends to accountability as well. It is generally agreed by the UN and ICRC that the state that deploys LAWS is responsible for its actions on the international stage. However, accountability should be articulated not just on the international stage, but in LAWS design processes as well.

Recommendations

International Legal Governance

The United Nations should facilitate new law that synthesizes and supplements existing international law in order to regulate LAWS. Data privacy, technology liability standards, and humanitarian law should be incorporated into LAWS regulation. This law should specifically define
LAWS, what constitutes the unethical deployment of LAWS, and anticipate future technological developments of LAWS. As many states as possible should be signatories to encourage international cooperation. To encourage participation, the UN should stress the need for safeguards against hijacking. States may be reluctant to cooperate given the military advantage LAWS offer; as such, non-proliferation should be incentivized by legal consequences for unethically deployed LAWS.

*States and State Militia*

States, regardless of their intent to participate in the LAWS arms race, should cooperate with other state actors on regional agreements. Data privacy regional agreements that articulate the permitted use of civilian data in wartime should be enacted to protect citizens. Non-proliferation should be encouraged among neighbors and adversaries to prevent the development of faulty LAWS or battlefield singularity.

*NGOs, Non-profits, and the Private Sector*

NGOs and nonprofits should continue to apply pressure on weapons manufacturers, states, and the UN to increase the ethical use of LAWS. Fully autonomous LAWS should be the focus of disarmament pressure, and human-controlled LAWS should be the focus of ethics campaigns. Scientists and business leaders should offer their expertise and opinions on LAWS and their ethicality.
Conclusion

LAWS, Lethal Autonomous Weapons Systems, are automated weapons with the intent to identify and engage targets in combat. These machines, particularly those remote-controlled or based on machine learning, are insufficiently regulated. Their use poses many ethical issues in humanitarian, technical, and legal principles that must be further articulated and discussed internationally before the arms race accelerates. Some call for their total ban, while others develop them full-steam ahead. Enforcing disarmament may prove difficult, but not impossible, as the nuclear arms race showed. Regardless, the first step for pro- and anti-LAWS groups should be to ensure their ethical use while they are in active combat use. Until such action is taken, human lives and the integrity of humanitarian law are at risk.
Works Cited


https://verfassungsblog.de/data-protection-in-armed-conflict/


Geneva Conventions and their Additional Protocols. 


International Committee of the Red Cross. “Military Necessity.”

https://casebook.icrc.org/glossary/military-necessity#:~:text=The%20%E2%80%9Cprinciple%20of%20military%20necessity,prohibited%20by%20international%20humanitarian%20law


https://thebulletin.org/2021/05/was-a-flying-killer-robot-used-in-libya-quite-possibly/


https://www.logostech.net/birth-of-wami_isr/. For more on WAMI, see:


https://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=2&psid=3062#:~:text=One%20reason%20why%20the%20Civil,quarter%20of%20a%20mile%20away


https://www.aptiv.com/en/insights/article/what-is-sensor-fusion#:~:text=Sensor%20fusion%20is%20the%20ability,strengths%20of%20the%20different%20sensors


