OF ROBOTS AND RULES: AUTONOMOUS WEAPON SYSTEMS IN THE LAW OF ARMED CONFLICT

MICHAEL PRESS*

ABSTRACT

In September 2016, hoping to quiet fears about “killer robots,” then-Defense Secretary Ashton Carter promised that whatever weapons systems the United States might develop in the future, “there’s always going to [be] human judgment and discretion.” Carter’s policy assurance on the future development of autonomous weapons systems (AWS) was clearly informed by ethical considerations, but it also had a distinct basis in the law of armed conflict (LOAC), embodied in various international treaties. This Note will conduct an analysis of the legal regime surrounding the construction and use of these AWS. In order to do so, it will examine similar weapons systems utilized by the U.S. military in various operations across the globe and current U.S. doctrine on the use of robotic autonomy in weapons, as well as the arguments for and against their fielding. An overview of LOAC and international humanitarian law (IHL) principles will also be explored through a clearly articulated legal review that should be undertaken before any weapon is legally allowed to operate in a battlespace. Subsequently, that legal review will be applied to AWS to investigate whether these weapons systems should be legally prohibited and how certain uses should be restricted. This Note asserts that there is nothing from a legal perspective that fundamentally prohibits the use of AWS in combat situations. However, similar to other weapons, it is the implementation of AWS that could come into conflict with LOAC and IHL. Recommendations for creating and using AWS in line with international legal principles will be interspersed throughout the Note and summarized in the conclusion. Key recommendations include limiting the use of AWS to situations where a system can reliably and predictably abide by the core principles of LOAC, as well as establishing standards and guidelines to ensure that AWS are fielded in such a manner.


I. INTRODUCTION ........................................... 1338
II. CURRENT U.S. AWS DOCTRINE, AWS DEBATE, ANDFIELDED
    SYSTEMS ............................................. 1339
III. INTERNATIONAL LAW AND LEGAL REVIEWS OF WEAPONS ....... 1345
    A. Weapons Law Overview .............................. 1347
    B. Targeting Law Overview ............................. 1348
    C. Accountability Overview ............................. 1352
IV. LEGAL REVIEW APPLIED TO AWS ............................ 1353
    A. Legal Review Applied to AWS—Weapons Law .......... 1354
    B. Legal Review Applied to AWS—Targeting Law ........ 1356
    C. Legal Review Applied to AWS—Accountability .......... 1362
V. CONCLUSION/RECOMMENDATIONS ............................. 1365

I. INTRODUCTION

History is filled with examples of how the integration of new technologies drastically affects the outcome of a conflict. Such technologies have not only been used to destroy more efficiently and abundantly, but also to defend people from harm. Since the longbow gained prominence at the Battle of Agincourt in 1415 through the advent of the atomic bomb at Hiroshima and Nagasaki in 1945, the necessity to be victorious in warfare has truly proven to be the mother of invention.

However, in the modern era, as technology enabled the destruction of combatants and non-combatants at levels not seen previously in human history, agreements among nations to ban or limit the use of certain technologies in hostilities began to take root. Examples of this restraint can be seen in the Chemical Weapons Convention (CWC) and the Ottawa Treaty banning the use of anti-personnel mines.\(^2\) The law of armed conflict (LOAC) and international humanitarian law (IHL), which many of these agreements crystallize, further moderates which weapons are considered legal in conflicts and regulates their use. Given the pace of technological advancement, weapons systems with sophisticated autonomous technology that do not require humans for targeting and firing decisions could soon be introduced to the battlefield. When these systems become available, IHL or LOAC issues may emerge that could limit the United States and other countries in their use of these fully autonomous weapons systems (AWS).

In order to conduct an analysis of any such limitations, this Note will discuss similar weapons systems currently in use by the United States, current U.S. doctrine on the use of robotic autonomy in weapons, as well as the benefits of such autonomy, and organizations who argue against their fielding. An overview of LOAC and IHL principles will also be explored in the form of a legal review that should be undertaken for all weapons before they are legally allowed to operate in a battlespace. Subsequently, the legal review involving certain IHL/LOAC principles and concepts will be applied to AWS to investigate whether they are legally prohibited as well as how certain uses should be legally restricted. Recommendations for the regulation of AWS will be interspersed throughout the Note, and summarized in the conclusion.

II. CURRENT U.S. AWS DOCTRINE, AWS DEBATE, AND FIELDED SYSTEMS

The U.S. Department of Defense (DoD) defines AWS, also referred to as lethal autonomous weapons systems (LAWs), as a weapons system that “can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapons systems that are designed to allow human operators to override operation of the weapons system, but can select and engage targets without further human input after activation.” In simplistic terms, AWS are pre-programmed not to need a human behind the controls in order to shoot, move, or communicate when engaging an enemy—the very basic elements of tactical combat. Yet, AWS should also have the ability to decide if an entity is an enemy target that can even be engaged, based on its programming parameters. Whether operating in the air, on land, or in water, the technology to develop and build AWS, in some manner, already exists today. For example, current weapons systems, such as the Phalanx and Aegis naval defensive systems, exhibit autonomy, but still have human supervision.

Deep integration of autonomous systems is key to the DoD’s Third Offset Strategy, a long-term plan to develop and produce technologies for the U.S. military to ensure the United States maintains military superiority in all five domains of war (land, air, water, space, cyber) for

---


the next thirty to forty years. Former U.S. Deputy Secretary of Defense Bob Work emphasized the importance of autonomous systems to the DoD’s future, stating, “The Third Offset is really kind of simple at its core. It basically hypothesizes that the advances in artificial intelligence and autonomy—autonomous systems—is going to lead to a new era of human-machine collaboration and combat teaming.”

Central to the U.S. Government’s (USG) stance on AWS is its current policy, specified in DoD Directive 3000.09, November 2012. The policy “establishes guidelines to minimize the probability and consequences of failures in autonomous and semi-autonomous weapons systems that could lead to unintended engagements.” In effect, the directive bans the development of AWS that are specifically designed to operate without a human able to override a targeting solution the system may make. However, because the directive describes policy not mandated by specific legislation, the ban can be amended if the DoD, with guidance from leadership in the executive branch, decides to begin such development. Additionally, the directive will automatically expire in 2022, prompting a reevaluation in the halls of the Pentagon, White House, and Congress if having offensive AWS would be a worthwhile endeavor.

Currently, the U.S. military does field defensive AWS, such as the Aegis at sea and the Patriot on land, both designed to shield against missile attacks. These two systems, in addition to others, such as the C-RAM and Phalanx, are meant to counter an incoming threat to U.S. forces. For instance, maritime Phalanx and its land-based equivalent C-RAM, are both designed to identify, confirm, and defend a ship or a base from incoming offensive weapons such as missiles, artillery, and rockets. While both systems have proven their worth in combat, during the Persian Gulf War in 1991, a Phalanx on autonomous mode


6. Id.

7. See DIRECTIVE 3000.09, supra note 3, at 1.


9. See id.


11. Id.

12. See id.
on the USS Jarrett mistakenly fired at a countermeasure fired by the USS Missouri.\footnote{13} The incident resulted in four depleted uranium 20-MM rounds impacting the Missouri, with minimal injuries and damage.\footnote{14} Similar actions by a Phalanx had not been seen prior to the incident and it was written off as a system malfunction.\footnote{15} However, a theory still persists that the friendly fire was due to a Phalanx human operator firing the rounds, not the autonomous system itself, although no evidence of this exists.\footnote{16} While there have been further incidents where the Phalanx and Aegis have mistakenly fired at targets, none occurred as a result of autonomous feature malfunction.\footnote{17} Instead, human error in multiple areas was to blame.\footnote{18}

While ostensibly autonomous, human supervision is necessary in the targeting and firing activities of these defensive systems, in line with Directive 3000.09.\footnote{19} This supervision has seemingly curbed debate on their legality. As the ICRC points out on the defensive role and supervision of current autonomous systems such as the Aegis:

The ability to effectively control these weapons and the use of force seems to be closely linked to their predictability and reliability, as well as to strict operational constraints with respect to the task carried out, the targets attacked, the operational environment, the geographical space and time of operation, the scope to enable human oversight of the operation of the weapon system, and the human ability to deactivate it if need be.\footnote{20}

\begin{footnotes}
\item[14] Id.
\item[16] Id.
\item[17] Probably the most famous incident involving the Aegis is the downing of an Iranian civilian jetliner in 1988 by the USS Vincennes due to the crew’s misidentification of the plane as a fighter jet. Yet, the system’s autonomous capabilities were found not to be to blame; human factors instead were blamed. Additionally, a human operator was to blame when a Phalanx on a Japanese ship inadvertently shot down a U.S. jet it was training with. \textit{But see Jeremy Pitt et al., This Pervasive Day: The Potential and Perils of Pervasive Computing} 231 (Jeremy Pitt ed. 2012); Melissa Healy, \textit{Pentagon Clears Vincennes’ Crew: Report Cites Navy Errors in Airliner Tragedy but Blames Actions by Iran}, L.A. TIMES (August 20, 1988), \url{http://articles.latimes.com/1988-08-20/news/mn-572_1_crew-member}.
\item[18] \textit{See} Pitt et al., \textit{supra} note 17, at 231; Healy, \textit{supra} note 17.
This type of human control is referred to as “man on the loop,” meaning a human is not needed to make a firing decision, but can override an AWS decision at any time, which differs from “man in the loop,” which indicates the need of a machine to await a human decision before firing, as is the case with unmanned combat aerial vehicles (UCAVs), also colloquially referred to as “drones,” such as the MQ-1 Predator.21 “Loop” refers to the OODA (observe, orient, decide, and act) targeting decision loop.22 Directive 3000.09 currently creates a ban on what is referred to as “man-out-of-the loop” decision-making by an AWS, where a human is not supervising an AWS’s targeting/firing decision.23 It is exactly this last type of decision process that brings up the most contentious IHL and LOAC issues in regards to AWS.

AWS offer numerous and undeniable advantages compared to manned or unmanned systems. In addition to the fact that AWS would operate in environments where electronic warfare could jam or even hijack the communications uplink between a UCAV and its human operator, fielded AWS would theoretically react faster and multitask better than humans in the fast-paced, ever changing battlefield environment of the modern cyber age.24 This cognitive advantage would supplement the advantages that UCAVs currently offer, such as removing the human operator from the danger of a combat environment.

Additionally, UCAVs are able to do intensive tasks for longer periods of time because they do not have to return to base to relieve humans from the physical and mental stresses combat missions inflict.25 This ability to stay operational for longer periods allows UCAVs, and therefore AWS, to provide surveillance and loiter over possible targets longer and to incur more risks with the aircraft to ensure the proper identification of a target in order to ensure collateral damage is minimally incurred.26 The final report of the Defense Science Board


22. Created by U.S. Air Force Colonel John Boyd to describe his experience as a fighter pilot in the Korean Conflict, a model of the loop can be found at The OODA Loop, http://www.danford.net/boyd/essence4.htm.
23. Toscano, supra note 21, at 195.
Task Force on the Role of Autonomy in DoD Systems states: “[T]he true value of these systems is not to provide a direct human replacement, but rather to extend and complement human capability by providing potentially unlimited persistent capabilities, reducing human exposure to life threatening tasks, and, with proper design, reducing the high cognitive load currently placed on operators/supervisors.” Moreover, similar to unmanned systems, AWS could replace humans in certain dangerous combat situations, thus reducing the casualties of military personnel employing the system. This replacement could allow militaries to be more creative in their use of AWS in order to preserve human life.

As the use of UCAVs has expanded, a growing number of international humanitarian organizations have questioned their legality, as well as the introduction of AWS more generally. These organizations have already begun circulating to governments a draft for an international ban on the development of AWS. For instance, in an August 2017 open letter to the United Nations Convention on Certain Conventional Weapons (CCW), artificial intelligence leaders, including billionaire Elon Musk, predicted “a third revolution in warfare” if offensive AWS are allowed to develop, calling on the world body to add AWS to the list of weapons already banned by the CCW. This follows a 2015 letter signed by over 1,000 technology experts, scientists and researchers, including Stephen Hawking, Apple co-founder Steve Wozniak and Mr. Musk, warning about the dangers of AWS.

While the legality of UCAVs is not an issue that will be explored within this Note, the use of a weapons system with autonomous technology may represent a significant departure from other systems, considering that humans may not necessarily be involved in the decision-making process of a weapons system with autonomous technology. This development is significant enough to bring the legality of such use into question. Therefore, if the United States, a nation that arguably has

27. Id.
31. Id.
32. For more information on the United Nation’s own views on the legality of UCAV’s, see generally Christof Heyns (Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions),
the most technologically advanced military in the world, sought to develop and integrate AWS that would operate without human decision-making, such a move could result in major legal concerns within the international community.

Several non-governmental organizations have been established specifically to advocate for an international prohibition on AWS technologies, the most prominent being the International Committee for Robots Arms Control (ICRAC). The Campaign to Stop Killer Robots, of which ICRAC is a member, is an overarching organization comprised of like-minded organizations that also advocate for a ban, such as Human Rights Watch (HRW). Through ethical debates on the use of AWS, these groups have put forth legal bases for why there should be an international prohibition on the very development of AWS. Their legal arguments are focused on a belief that the technology necessary to develop offensive autonomous systems, which do not require humans for targeting/firing decisions, can never assuredly abide by certain precepts that provide the very foundation of LOAC and IHL. They contend that no matter how AWS are developed, these “killer robots [...] would lack human judgment and the ability to understand context.” Even the International Committee of the Red Cross (ICRC), which has a special role of monitoring the conduct of nations regarding IHL, has concerns with AWS. It has convened meetings to discuss limits needed on autonomous weapons systems to ensure they will predictably and reliably abide by IHL and LOAC.

In ICRAC’s opinion, the only manner in which LOAC principles, such as distinction, military necessity, unnecessary suffering, and proportionality, can be upheld at a reasonable level is by humans making

Ref. on the Extrajudicial, Summary or Arbitrary Executions, U.N. Doc. A/HRC/23/47 (Apr. 9, 2013) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_en.pdf (describing how UCAVs, per se, do not violate international law, but are akin to cruise missiles and other manned combat aircraft whose existences are not seen as violating international law, but whose uses in certain contexts could make them illegal in specific instances).

33. The Problem, CAMPAIGN TO STOP KILLER ROBOTS (July 22, 2016, 4:14 PM), http://www.stopkillerrobots.org/the-problem/ [hereinafter CAMPAIGN TO STOP KILLER ROBOTS].

34. See id.

35. See id.

36. See id.

37. See id.

38. See VIEWS OF THE INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) ON AUTONOMOUS WEAPON SYSTEM, supra note 20, at 3.
the ultimate decision to fire weapons on a certain target. While the ability of AWS to ever have the cognitive abilities to abide by such principles is unknown, these organizations offer an additional legal argument for why AWS should be prohibited: accountability. Who exactly would be accountable if AWS do violate LOAC/IHL? While possibilities involve the military commander, the programmer, or the manufacturer, those in favor of the ban believe that there could be instances when no one could be held accountable because none of these actors are actually making the decision to fire on a target. Although there is nothing in LOAC/IHL that states one must be held for accountable for violations, ICRAC and other organizations uphold that accountability is integral to LOAC by providing some justice to victims, punishing guilty offenders, and deterring others from committing LOAC/IHL violations. The viability of LOAC and IHL to protect certain classes of persons on the battlefield could be at risk because AWS could subvert the ability to place legal responsibility on an offender. These concerns raised by civil society regarding the potential dangers of offensive AWS are particularly important to address as interest, investment, and research in these weapons systems increase.

III. INTERNATIONAL LAW AND LEGAL REVIEWS OF WEAPONS

Integration of AWS that would be offensive in nature—for example, a system designed to take the place of a UCAV or even a soldier in the field—must be lawful under IHL in two distinct areas: weapons law and targeting law. Article 36 of Additional Protocol I (1977) of the 1949 Geneva Conventions, also known as AP I, describes what constitutes a legal weapon in IHL. Many contend that Article 36 simply crystallizes customary international law (CIL) and therefore all nations, whether signatories of AP I or not, are obligated to conduct such legal reviews. While the United States is not a signatory of AP I, the U.S. government

40. See id. at 29.
41. See id. at 42-45.
42. See id. at 45.
43. Id.
45. See LOSING HUMANITY, supra note 39, at 21-22.
recognizes that Article 36 and approximately two-thirds of the protocol is found in CIL.\(^{46}\) Therefore, the United States accepts the Article 36 obligation to evaluate a new weapon system’s legality. Article 36 states:

In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.\(^{47}\)

Formalizing CIL, Article 36 requires each nation to determine whether any new “weapon, means, or method of warfare” that it seeks to use, in some or all circumstances, is prohibited by international law.\(^{48}\) The review is multidisciplinary, “including military, legal, environmental and health-related considerations.”\(^{49}\) Legal reviews prior to development, through interaction with engineers, help avoid spent costs in money and manpower on weapons or functions that may later be found to be banned by international law.\(^{50}\)

U.S. policy is to review all weapons and their delivery systems, as well as any significant modification of them, through two legal reviews, one prior to formal development, and another before a weapon enters service by military personnel.\(^{51}\) Aside from the “weapons review” meant to determine whether a weapon fundamentally violates LOAC and therefore cannot not be fielded in any combat situation, international


\(^{47}\) See AP I, supra note 44, at Art. 36.


\(^{49}\) See id. at T-12.

\(^{50}\) See Schmitt & Thurnher, supra note 10, at 271.

law additionally calls for a “targeting review” of a weapon system.\textsuperscript{52} Targeting review involves reviewing distinct situations in which the use of the weapon system would violate principles of LOAC and limiting the weapon’s use in order to be in compliance with LOAC.\textsuperscript{53} Additionally, and somewhat unique with the advent of AWS, is an accountability overview—necessary to the investigation of possible liability for a LOAC violation.\textsuperscript{54}

A. Weapons Law Overview

The international community assesses such legal weapons reviews in two distinct areas. The first area, known as “weapons law,” consists of analyzing a weapon in three capacities: if its design inherently allows it to strike legitimate targets (combatants, military objectives) and illegitimate targets (civilians, civilian objects) without distinction; if its only use is to inflict “unnecessary suffering”; and if certain international agreements to which a state has voluntarily entered prohibit such a weapon.\textsuperscript{55} If a weapon violates any of these factors, based on its “normal or expected use,” it is illegal \textit{per se}, because there are no situations on the battlefield where it will not violate one or more of these factors.\textsuperscript{56}

A weapon is considered to lack the ability to discriminate between legal and illegal targets if it cannot be aimed at a specific target. The assessment factors include the accuracy and reliability of its targeting, the type of munitions used, and the area covered by the weapon.\textsuperscript{57} This principle of discrimination, also known as distinction, also involves prohibiting weapon systems that have uncontrollable effects despite their ability to strike a target accurately.\textsuperscript{58} Biological weapons and chemical weapons are classified as indiscriminate in this manner because their effects cannot be readily controlled and their virulence could spread to illegal targets (e.g., civilians, sick or wounded combatants).\textsuperscript{59}

Also prohibited under weapons law are weapons that cause “unnecessary suffering or superfluous injury.”\textsuperscript{60} This principle of unnecessary

\textsuperscript{52} See \textit{Losing Humanity}, supra note 39, at 21-22.
\textsuperscript{53} See \textit{LOAC Deskbook}, supra note 51, at 133.
\textsuperscript{54} See \textit{Losing Humanity}, supra note 39, at 42.
\textsuperscript{55} See id. at 30-31.
\textsuperscript{56} See Lawland, \textit{supra} note 48, at 10.
\textsuperscript{57} See \textit{AP I}, supra note 44, at Art. 51(4)(c).
\textsuperscript{58} See id.
\textsuperscript{59} See Toscano, \textit{supra} note 21, at 207.
\textsuperscript{60} See \textit{AP I}, supra note 44, at Art. 35(2).
suffering seeks to limit the ability of adversaries to adopt certain “means of injuring the enemy.”\textsuperscript{61} Examples of such prohibited weapons that are specifically designed to unnecessarily aggravate suffering or injury.\textsuperscript{62} Whether a weapon is specifically intended to cause “unnecessary suffering or superfluous injury” rests in large part on whether the suffering or injury is meant to serve a legitimate military purpose, such as attrition of enemy combatants, rather than a goal based on human emotion, such as vengeance.\textsuperscript{63} The third area for investigation is whether a new weapon is prohibited in some manner by previous agreements or specific treaty prohibitions. For example, the 1980 Certain Conventional Weapons Treaty prohibits certain booby traps, blinding lasers, and non-detectable fragments in conflicts.\textsuperscript{64} Additionally, the development, production, and stockpiling of biological and chemical weapons are prohibited through the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).\textsuperscript{65} While such weapons or their uses could be prohibited because they may violate the two prior criteria, there could be certain weapons that countries voluntarily enter into agreement to stop producing or using, despite their production or use not violating international law. For example, in the Strategic Arms Limitation Treaty II, the United States agreed to stop producing new land-based intercontinental ballistic missile launchers despite the fact that international law did not necessitate such a prohibition.\textsuperscript{66}

\textbf{B. Targeting Law Overview}

Even if a weapon or its associated delivery system is in accordance with “weapons law,” it must then be reviewed under a second area of the law, so-called “targeting law.” This area is more concerned with the conduct of hostilities and the circumstances of a weapon’s use, or \textit{jus in

\textsuperscript{61} See Kastan, \textit{supra} note 24, at 56.

\textsuperscript{62} See LOAC Deskbook, \textit{supra} note 51, at 153; see Schmitt & Thurnher, \textit{supra} note 10, at 244-45.

\textsuperscript{63} See Kastan, \textit{supra} note 24, at 56.

\textsuperscript{64} See LOAC Deskbook, \textit{supra} note 51, at 153.


Targeting law differs from weapons law in that targeting law governs the use of weapons in conflicts, but with restrictions pursuant to certain principles and articles of LOAC and IHL. Put simply, targeting law deals with the methods of warfare while weapons law deals with the means of warfare. Nevertheless, principles such as distinction, which are found in weapons law, are also found in targeting law, but are applied in a “use” context. Additionally, there are various international agreements and treaties that countries enter into that restrict the use of certain weapons in certain contexts, such as Protocol II of the CCW that regulates the use of land mines.

As in weapons law, targeting law requires a review of discrimination in terms of the specific environments or situations in which a weapon system can be operated. For a weapon to be used in accordance with the principle of distinction under targeting law, it can only be used in situations that allow for targets to be reasonably distinguished between legal and illegal, and not in situations where such distinction cannot be made. This differs from weapons law because a weapon in targeting law may be able to distinguish between legal and illegal targets in some situations, but not others. The weapon would only be able to be utilized in those specific scenarios where it could reasonably distinguish between combatants and civilians (or other illegal targets).

The principle of military necessity, crystallized by Article 52(2) of the AP I, dictates that targets are “limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.” In summary, necessity means that weapons must be tailored to apply only the force necessary to achieve a legitimate military objective, with legitimacy of a military objective dictated by the

---

68. Id.
69. See id. at 247.
71. See Toscano, supra note 21, at 210.
72. See id.
73. See id.
74. See id.
75. See AP I, supra note 44, at Art. 52(2).
advantage it provides in defeating the opposing military force. This is significantly related to the “unnecessary suffering” factor of weapons law, because both involve judging if a weapons impact would result in a military advantage.

Proportionality is another important principle under targeting law. It deals with the amount of force to be applied to a target to achieve a legitimate military advantage, with the least amount of collateral damage necessary. Differing from necessity, which is almost a qualitative assessment to determine if force against a target would achieve a military advantage, proportionality involves a more quantitative assessment to determine the right amount of force needed to achieve nothing more than the military advantage sought. For example, in an urban environment, certain indirect weapons, such as artillery, may be restricted because the damage that would result from destroying an enemy target in a populated area could also include the excessive death and destruction of civilians and civilian infrastructure. Yet, in an unpopulated area where a reasonable individual would not think civilians live, an artillery barrage or airstrike would be allowed. Consequently, proportionality must take into account the importance of the military advantage sought versus the calculation of civilian damage anticipated with the use of a certain weapon. Key to this assessment is establishing whether the collateral damage inflicted by a weapon would be “excessive.” The greater a military advantage anticipated through a weapon’s use, the more collateral damage tolerated under LOAC/IHL. Therefore, a weapon’s use that results in civilian deaths, even if foreseen, would not always violate the principle of proportionality based on the significance of the military advantage gained. This idea is encapsulated in the U.S. justification for unleashing the atomic bomb over Hiroshima and Nagasaki in 1945. While highly debated even in the present, the considerable advantage the United States sought—notably the unconditional surrender of the Empire of Japan and the elimination of the need to stage a military invasion of the Japanese

76. See Kastan, supra note 24, at 55.
77. See Toscano, supra note 21, at 211.
79. Id.
80. This subjective element of proportionality is very divisive, because it is based on a “reasonable commander” in a very specific situation. As a result, much criticism is heaped on proportionality whenever military operations result in the death of civilians, whatever the amount, and such deaths were anticipated by commanders, see Schmitt & Thurnher, supra note 10, at 254 (2013).
home islands—justified, in its view of LOAC, the dropping of both bombs despite the considerable civilian casualties that resulted from the decimation of the cities.  

Finally, feasible precautions must be taken when operating weapons, based on reasonability. Feasible precautions require combatants to “do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and . . . are military objectives.” This also involves taking precautions in “avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.”

There is debate in the LOAC and IHL communities regarding what “everything feasible” actually entails due to the fact that not conducting an attack that might kill civilians could arguably be a feasible precaution. However, this line of thinking conflicts with AP I and CIL—as mentioned previously, principles such as necessity and proportionality allow for civilian deaths in some instances. The DoD expresses its understanding of “feasible” in its 2015 Law of War Manual by equating the word with “practicable,” “reasonable,” “due,” and “necessary.”

According to the Manual, “[t]he standard for what precautions must be taken is one of due regard or diligence, not an absolute requirement to do everything possible [but, only] those that are practicable or practically possible.”

Given this measure, such feasible precautions could involve halting or delaying the use of a weapon once it becomes clear that civilians would unnecessarily be killed, such as altering the flight path of a cruise missile when civilians unexpectedly enter the target zone, or by loitering over an area until civilians are not in danger, such as with manned


82. See AP I, supra note 44, at Art. 57(2).

83. Id.

84. See Schmitt & Thurnher, supra note 10, at 254.


86. Id. at 189-190.
or unmanned aerial vehicles.87 However, a soldier would not necessarily be guilty of not taking feasible precautions if she were to fire at a combatant who then moves out of the way, resulting in the death of an unseen civilian.88 Despite the fact that the soldier did not delay her fire until the civilian moved out of harm’s way, if there were no indications that a civilian would be present behind the enemy, there would be no violation.89

C. Accountability Overview

Outside of weapons and targeting law reviews, there exists another aspect of law that may be unique to the legality of AWS— one that has largely been taken for granted in the history of IHL and LOAC until the advent of this technology.90 Accountability becomes an issue if any of the aforementioned weapons and targeting law principles are violated. LOAC and IHL transgressors are held culpable in order to punish the guilty, deliver some justice to victims, preserve LOAC, and regulate the methods and manner of war.91 AP I requires member states to prosecute those responsible for “grave breaches” of LOAC, no matter the nationality of the offender.92 World War II is seen as a foundational example in the punishment of “war crimes,” such as the Nuremberg Trials for Nazi war criminals, as well as the similar trials that took place in Japan for Imperial Japanese war criminals.93

Many of the violations that the offenders were accused of were not for violations they directly ordered, but instead for violations related to

87. The U.S. Tactical Tomahawk Command and Control cruise missile system allows for the operational commander to “receive real-time targeting coordinates and applying them to a tactical Tomahawk missile in flight” making it feasibly possible to avert a strike while in-flight. Yet, of course, necessity comes into play if the target was especially worth the loss of civilian life, see Staff Writers, Tomahawk Remote From 5,000 Miles Away, SPACE DAILY (May 20, 2010), http://www.spacedaily.com/reports/Tomahawk_Remote_From_5000_Miles_Away_999.html.

88. See LAW OF WAR MANUAL, supra note 85, at 189-91.

89. However, other information could come into play based on the context of the situation, resulting in a violation of a principle. For instance, while the civilian was unseen, if an area was known to be heavily populated, and perhaps a grenade, instead of a rifle was fired, this could result in the soldier violating IHL based on the principle of proportionality.


91. See id.

92. While the United States and a minority of countries have not ratified AP I, a majority of AP I is recognized as customary international law. See AP I, supra note 44, at Art. 85-86.

the concept of “command responsibility.”94 First codified in Art. 86 of AP I, command responsibility requires military commanders to prevent, suppress, and report breaches of IHL.95 The United States itself recognizes command responsibility in international law as seen in In re Yamashita, where an Imperial Japanese general was found to be culpable for the actions of his troops by the U.S. Supreme Court.96 While the defense claimed the general did not have knowledge of LOAC violations committed by his troops due to communication problems caused by ongoing hostilities with Allied forces, the Court nevertheless found he had “an affirmative duty to take such measures as were within his power and appropriate in the circumstances to protect prisoners of war and the civilian population.”97 In terms of weapons and command responsibility, Article 36 of AP I states that the potential for misuse of a weapon does not necessarily render that weapon system incompatible with IHL.98 Although, under Article 87, commanders must retain reasonable control of those weapons and their use by subordinates, it leaves open what actually constitutes “control.”99

IV. LEGAL REVIEW APPLIED TO AWS

While AWS may have tactical reverberations on the battlefield that have strategic implications on militaries that utilize or face these weapon systems, weapons law review and targeting review must still be applied to an AWS before it can be fielded in combat in accordance with LOAC and IHL. While AWS may perhaps spur an evolutionary leap in modern warfare, there is nothing inherent in these technologies that would result in them being in violation of weapons law. Moreover, in a targeting law review, AWS are comparable to other weapon systems in that limitations should be adopted to constrain their use to ensure they are used in conformance with international laws and customs. Additionally, because the use of AWS has brought into question who would be held responsible for a LOAC violation resulting from these systems, an accountability review seems appropriate. In conducting general research on what such an investigation into an AWS violation would entail, it appears likely that a human within the

94. See AP I, supra note 44, at Art. 87.
95. See id.
96. In re Yamashita, 327 U.S. 1, 16 (1946).
97. Id.
98. See AP I, supra note 44, at Art. 36.
99. See AP I, supra note 44, at Art. 87.
chain of command that allowed for its use in a combat situation or one responsible for the manufacture or upkeep of an AWS would be held accountable.

A. Legal Review Applied to AWS—Weapons Law

To legally integrate AWS into the U.S. military arsenal, a review of weapons law and targeting law must be applied to AWS. With regard to weapons law, there is currently no international treaty or ban that prohibits the fielding of AWS. While certain non-governmental organizations, such as Human Rights Watch and the International Committee for Robots Arms Control have banded together to encourage nations to adopt a preemptive prohibition on fully automated weapon systems without human control, known as the Campaign to Stop Killer Robots, the movement has not achieved its aim.100 Their goal of banning AWS is based on a belief that these weapon systems “would not only be unable to meet legal standards but would also undermine essential non-legal safeguards for civilians.”101 The legal principles that opponents of AWS believe would be violated have been mentioned previously in weapons and targeting law, but their opposition is also based on “non-legal,” or ethical, protections. These considerations include a supposed need to have human emotion present in an attacker to curtail killing and violating of LOAC.102 The Campaign seeks to ensure a direct human presence on the battlefield and to stop the further automation of conflict.103 This reduction in human involvement pur-

100. See Campaign to Stop Killer Robots, supra note 33. While there may currently be no global treaty prohibiting AWS, the policy adopted by the United Kingdom’s Ministry of Defence in September 2017 of restricting the possession and research of fully autonomous offensive weapons systems is evidence that there is a strain of belief in some national governments of a need to have a human behind the controls of weapons of war. Because the adoption of this policy is recent at the time of the writing of this Note, it is too soon to predict if this could start a global campaign of other nations unilaterally banning similar weapons in their militaries. See Dom Galeon, Following Elon Musk Letter, UK Government Plans to Ban Fully Autonomous Weapons, FUTURISM (Sept. 13, 2017), https://futurism.com/following-elon-musk-letter-uk-government-plans-to-ban-fully-autonomous-weapons/. However, it could be a means to such a ban as opposed to an international treaty. Id.

101. See Losing Humanity, supra note 39, at 1-2.

102. See id. at 31-32.

103. While these arguments are non-legal in nature and thus not particularly a focus of this Note, the emotion aspect can have a LOAC element if AWS being without emotion is seen as a feasible precaution. For example, the situation surrounding In re Yamashita involved subordinates’ own LOAC violations on civilians and prisoners of war, driven by human emotion. Human emotion can also be seen as partly responsible for many other war crimes from Yugoslavia to Rwanda. In this manner, having an AWS without emotion, but armed with programming that
portedly encourages political leaders in democratic nations to defer to using kinetic action at a higher rate, because the threat to their troops is greatly reduced, resulting in a lower number of casualties.\textsuperscript{104} With reduced casualties, the belief is that voters are less averse to war because of the fewer observable human costs, and thus unlikely to vote out of office politicians encouraging military use.\textsuperscript{105} The campaign currently is focusing its efforts on adopting an international AWS ban by attempting to integrate it into the CCW, which already bans other types of conventional arms, a strategy similar to what technologists such as Elon Musk are advocating.\textsuperscript{106}

Additionally, in March 2016, the U.N. Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions produced a joint report recommending an AWS prohibition for warfare and for law enforcement use because of the lack of human control.\textsuperscript{107} While some nations do support such a ban,\textsuperscript{108} they outwardly project other pragmatic reasons for desiring a prohibition, not simply for the same legal and ethical reasons of the campaign. For instance, some competitor nations that are not as technologically advanced as others, and thus probably would not have the ability to produce or attain AWS for years after other countries are able to integrate them into their arsenals, if ever, would be at a military disadvantage. Therefore an AWS prohibition would only aid these nations at a technological disadvantage by removing this capability enables it to abide by the LOAC principles, one could argue that it could be an obligation to not have an AWS with human emotion coding. Additionally, the argument that the replacement of combatants on the battlefield with machines makes war easier is also flawed. For instance, because the Taliban and Al Qaeda elements in Afghanistan and Pakistan have little to no anti-aircraft abilities, it makes no practical difference whether a manned or unmanned aircraft is conducting airstrikes, considering both are capable of completing their missions without engagement by the enemy. Precision long-range missile strikes, such as Tomahawk cruise missiles, have also been used for similar purposes, though have not received the same type of criticism. See id. at 37-39.

\textsuperscript{104} See id.
\textsuperscript{105} See id. at 39-40.
\textsuperscript{106} See Campaign to Stop Killer Robots, supra note 33; see Killer robots, supra note 30.
from more advanced nations.\textsuperscript{109}

In the absence of explicit international controls or restriction, AWS must be reviewed under existing weapons and targeting law. In contending with the discrimination element of weapons law, an AWS must be able to distinguish between legal and illegal targets when operating its actual weapon.\textsuperscript{110} Yet, if an AWS was only built to fire weapons that are prohibited by LOAC/IHL, such as chemical or biological weapons, such an AWS would be rendered illegal under weapons law, regardless of whether it could differentiate lawful from unlawful targets, because whenever such an AWS operates, it would operate illegal weapons.\textsuperscript{111} A similar conclusion is found when applying the principle of unnecessary suffering to AWS under weapons law to investigate if such weapon systems always result in superfluous injury needed to accomplish the military advantage sought. As long as AWS designers do not specifically create AWS that are only capable of operating munitions resulting in unnecessary suffering or superfluous injury, then such weapons systems would abide by this element.\textsuperscript{112} With that final assessment, there appears to be no inherent qualities within AWS that would prohibit their operation under international law within weapons law.

B. **Legal Review Applied to AWS—Targeting Law**

Under targeting law, there are no international treaties restricting certain legal uses of AWS, akin to regulations on the use of land mines, outside of those applied to all weapons and weapon systems under international law. A restriction on AWS could actually be a more viable alternative as opposed to a prohibition.\textsuperscript{113} This use limitation would be

\textsuperscript{109} From the overarching paradigm of the realist theoretical approach to international relations, a country would be motivated by national priorities of power and survival shrouded as moral causes in order to deny other states a capability that could threaten their standing or even existence in the international community. See generally \textsc{Jack Donnelly, Realism and International Relations} (Cambridge Univ. Press 2000) (2004).

\textsuperscript{110} Jeffrey S. Thurnher, \textit{No One At the Controls: Legal Implications of Fully Autonomous Targeting}, 67 \textit{Joint Forces Q.} 77, 80 (2012).

\textsuperscript{111} See Toscano, supra note 21, at 207.

\textsuperscript{112} Id.

\textsuperscript{113} Kenneth Anderson, Daniel Reisner, and Matthew Waxman’s \textit{Adapting the Law of Armed Conflict to Autonomous Weapon Systems}, argue for such a regulation and not a ban by first addressing how AWS are different as compared to other new weapon systems. Yet, while these differences are unique, the article advances legal reasoning that AWS can be regulated within the framework of existing LOAC. While there is potential for LOAC violations for AWS, AWS use can be tailored to ensure they are not inherently unlawful and that commanders use them in a manner consistent with LOAC, similar to a vast amount of other current weapon systems. The article also discusses
AWS IN THE LAW OF ARMED CONFLICT

preferable because of the benefits of AWS in war that would sway nations away from a ban and the benefits of guiding the evolution of AWS technology to ensure nations are aware they need to be tightly bound to established LOAC and IHL principles.114 A use limitation would also prove to be beneficial in order to close legal loopholes nations might use to subvert any ban, due to the enforceability hurdles and dangers of any attempt to prohibit AWS.115

Under distinction, AWS must have the capability to distinguish between civilians and combatants, the same as any weapon system. Additionally, if a combatant becomes wounded, an AWS must be able to recognize this, and realize that a wounded combatant is “immunized,” and not a legal target.116 The apparent difficulty in developing technology that can be comparable to a reasonable human’s ability to distinguish is a central argument of those advocating a ban.117 In their opinion, AWS “would not have the ability to sense or interpret the difference between soldiers and civilians, especially in contemporary combat environments.”118 Furthermore, as is often the case in modern warfare, the enemy does not always wear a uniform, making it difficult to determine who is a civilian or combatant, especially in the counterinsurgency environments of Iraq and Afghanistan.119 In addition, the emotional state of an individual on the battlefield could also be an indication of their intention and lead to their identification as enemy or civilian.120 Those advocating for an AWS ban argue all of these distinguishing features as obstacles that an AWS can never sufficiently address.121

weaknesses of a prohibition, such as reasons why there could be no bright-line standard for making all variations of AWS illegal, and that nations will find legal loopholes, making an international agreement on regulation of what capabilities would be illegal more practical. Finally, the article advances a three-tiered process for AWS regulation that integrates LOAC oversight at the international-, national-, and industrial-level; the three levels that have the most potential to affect the development and use of AWS and ensure they are coherent with LOAC. This approach has obstacles in itself to overcome, but the authors at least do confront these hurdles, if at least tangentially. Additionally, the article does not necessarily state that some type of human must be in supervision of AWS, as other means of regulation do purport, see generally Kenneth Anderson et al., Adapting the Law of Armed Conflict to Autonomous Weapon Systems, 90 Int’l L. Stud. 386 (2014).

114. See id. at 393.
115. See id. at 397.
116. See AP I, supra note 44, at Art. 10.
117. See LOSING HUMANITY, supra note 39, at 4.
118. See id. at 30.
119. Id.
120. See id. at 31-32.
121. See Andersen et al., supra note 113, at 395.
However, simply because the technology necessary to abide by LOAC is far from completion does not mean that it will never exist. The sensors needed to abide by LOAC must not be perfect in terms of distinction to be lawful under targeting law. The standard is reasonableness. Therefore, if it would be reasonable for a human, under certain circumstances, to fire on a target that turns out not to be valid, neither the human, nor an AWS under similar circumstances, would be found to violate LOAC. Additionally, while the lack of emotion has been proposed as a reason why AWS should not be fielded because they could not identify such emotion, this could actually be an advantage. AWS’s lack of fear means that AWS can put themselves more at risk of a surprise attack, even sacrifice themselves, in order to identify if a possible target is legitimate.

Military necessity as it pertains to AWS is intricately tied to discrimination. To determine if the destruction of a target offers some military advantage, the standard for determining necessity, an AWS would need to first determine that the target is legitimate. However, if distinguishing a legitimate target is currently a technological hurdle, determining military advantage would be even more intensive. Such a determination would involve AWS programming of a commander’s Rules of Engagement (ROE), escalatory steps that a commander’s subordinates are obligated to abide by based on context-specific combat situations in order to limit death and destruction to necessary times. Yet, if technological advances can be successfully achieved in an AWS, within reasonable rates of error comparable to the reasonability found in distinction, an AWS could be acceptable under LOAC.

Akin to military necessity, proportionality would mandate that AWS have technology that allows it to assess the military advantage gained versus the amount of civilians and civilian infrastructure destroyed by a possible attack. As mentioned previously, because self-preservation could be explicitly excluded from the programming of AWS in specific scenarios, AWS teams could even probe further into an enemy’s midst to investigate if such an attack would be proportional, or even hold off returning fire until it can reasonably assess proportionality criteria.

122. *See* Thurnher, *supra* note 111, at 77.
123. *See* Andersen et al., *supra* note 113, at 393.
124. *Id.*
125. *See* Thomas, *supra* note 67, at 266.
Reasonability is key in a decision as to whether the military advantage gained is worth civilian destruction to proportionality. With this lack of a self-preservation instinct, AWS can be used to gather further evidence in deciding if an attack is reasonable under the circumstances or not, similar to UCAVs. However, unlike UCAVs where a human is behind a targeting decision, AWS would lack the emotional complexity that can skew human estimates of whether the collateral damage predicted is worth the military advantage to be gained.

Similar to arguments that AWS could never abide by distinction and other LOAC principles, ICRAC and other organizations contend that proportionality is “abstract, not easily quantified, and highly relative to specific contexts and subjective estimates of value.” Proportionality involves understanding the context of a situation. It is improbable, in their view, that an AWS could ever have the technology to sufficiently be able to comprehend all the possible scenarios one finds on the battlefield. If an AWS cannot understand the context of a distinct situation, it does not have the tools needed to assess proportionality when targeting.

These are important considerations, though proportionality does involve quantitative calculations to a certain extent, and coding for the AWS could build in quantitative assumptions, controlling for a certain degree of subjectivity and helping to establish a proportionality estimate. In a simplistic example, if an AWS is programmed with the lethal radius of its on-board weapon, where anything within that radius would take substantial damage, and there are a certain number of civilians identified within that radius, an AWS could halt firing. Additionally, different targets could be assigned a priority in the AWS programming with a certain assumption of how much expected collateral damage an AWS is allowed to accept when firing, based on the military advantage gained. Similar software is already used by U.S. military analysts in determining whether possible airstrike targets on the ground comport with proportionality.

129. See Toscano, supra note 21, at 211.
130. See Thomas, supra note 67, at 268-69.
132. See LOSING HUMANITY, supra note 39, at 32-33.
133. See id. at 33.
134. See Schmitt & Thurnher, supra note 10, at 256.
135. The DoD and CIA utilize a computer program named “Bugsplat,” later renamed “Fast Assessment Strike Tool — Collateral Damage” (FAST-CD), since at least 2003 for calculating and reducing collateral damage resulting from airstrikes, see Bradley Graham, Military Turns to Software to Cut Civilian Casualties, WASHINGTON POST (Feb. 21, 2003), https://www.washingtonpost.com/archive/politics/2003/02/21/military-turns-to-software-to-cut-civilian-casualties/af3e06a3-e2b2-4258-b511-31a3425bde31/.
For example, a mortar team in a heavily populated civilian area may not be able to be engaged by an AWS with a high-explosive weapon, such as a Hellfire missile or return mortar fire, but it could engage with an on-board 30-MM machine gun with a far less lethal radius. In addition, perhaps engaging a mortar team with a Hellfire missile would not yield the military advantage worth the collateral damage accepted, but engaging a top-level leader of an enemy force could be worth the collateral damage expected for the military advantage gained.

Feasible precautions are critical to ensuring AWS reasonably abide by LOAC principles. This guarantees that the AWS technology is up to the task of abiding by LOAC in a multitude of situations, akin to the situations a human would find herself in. Rigorous testing and evaluation prior to, and even after, fielding AWS is thus crucial from a precautionary standpoint.136 While the feasibility of certain precautions is very subjective, there are options commanders and programmers can make to lessen the ability for AWS to violate LOAC principles. For instance, in addition to software that enables an AWS to distinguish targets, and to evaluate necessity and proportionality, an AWS could also be programmed to operate or fire only within a certain geographic area. This programming constraint could ensure that collateral damage is not sustained in heavily populated civilian areas.137

An AWS could also only be armed with lower lethal radius weapons, such as machine guns instead of higher lethal radius direct weapons, like missiles, or indirect weapons, such as grenades or mortars. This would help reduce collateral damage issues. Additionally, an AWS could be programmed to either automatically return to base, shut-down, or even self-destruct if its systems register a critical failure in its processing or is active for a period longer than its systems are pre-programmed to be active for.138 AWS use could also be restricted initially to conventional, state vs. state conflicts, where there are forces wearing identifiable uniforms, and utilizing distinct weapons and vehicles. Such visualizations would enable an AWS to better determine friend, foe, or civilian, just as it is easier for humans to distinguish in such environments, rather than irregular warfare where such distinctions are less straightforward.139

Moreover, human supervisors could monitor AWS remotely. While similar to UCAV remote pilots, remote supervisors would not be “in”
the targeting loop, meaning their decisions would not be needed in order for on-board weapons to operate on a certain target. Instead, remote supervisors would be “on” the targeting loop, where they could monitor the target selections of AWS, and override a targeting decision by an AWS. Such human/AWS interaction could allow for the legal fielding of AWS. The U.N. Special Rapporteur on the extrajudicial, summary or arbitrary executions, Christof Heyns, indicated as much when he stated, “[w]hile it is not clear at present how [AWS] could be capable of satisfying IHL and IHRL requirements in many respects, it is foreseeable that they could comply under certain circumstances, especially if used alongside human soldiers.” Additionally, the DoD’s 2015 Law of War Manual recognizes that such supervision of an AWS could be required to decrease the likelihood of collateral damage because of the complexity of the technology. Furthermore, AWS could initially be reserved only for specific missions where civilians would reasonably not be present, such as a military base in an austere environment not surrounded by a civilian population.

While this supervision restriction could appease some who have legal objections to AWS, it would be counterintuitive to some of the benefits of such a system. First, the continued integration of technology into warfare means that the speed of combat is becoming faster, outpacing the abilities of humans to accurately react in a timely manner. AWS are meant to deal with this ever-increasing tempo. Thus, any supervision may eventually become superfluous because a human may not be able to comprehend the high pace of combat. In addition, electronic warfare will continue to be more proficient at interrupting the communication link that would connect the remote supervisor with the AWS, even making such a constant uplink a pathway for hacking AWS by “spoofing,” or tricking, AWS to interpret navigation signals differently.

Finally, an AWS’s decision software could be more logical than its human supervisor’s. This could lead to a human’s inability to

---

140. See Toscano, supra note 21, at 213.
141. See Heyns, supra note 32, at 20.
142. See LAW OF WAR MANUAL, supra note 85, at 330.
143. See Toscano, supra note 21, at 210.
144. Less sophisticated UAVs utilizing GPS are prone to such spoofing, but spoofing possibly contributed to the capture of the stealth U.S. RQ-170 Sentinel UAV in Iran in 2011. See Bob Orr, U.S. official: Iran does have our drone, CBS NEWS (Dec. 8, 2011), http://www.cbsnews.com/news/us-official-iran-does-have-our-drone/. Furthermore, Shi’ite insurgents in Iraq, while not able to take control of a UAV, repeatedly intercepted live video feed from a U.S. UAV, unbeknownst to technicians, using only $26 worth of equipment. The resulting extra encryption needed to protect the feed has possibly slowed the ability to share and analyze the data within the DoD and with
properly comprehend the facts causing an inadvertent attack on an illegal target, or emotional judgments interfering with a logical determination.145 Yet, given these reasons as to why a remote supervisor would be at a disadvantage to AWS, such a precaution could ameliorate many of those who have ethical and legal arguments against AWS, especially when they are initially fielded. Therefore, while there are many ways in which the use of AWS could violate targeting law, if sensible limitations are placed on specific weapons systems in order for it not to be used in an illegal manner, AWS would abide by targeting law.

C. Legal Review Applied to AWS—Accountability

Many opponents of AWS base their call for a prohibition on the fact that these systems would be unique and their use could result in LOAC violations for which no one could be held accountable.146 In many ways, this is more of an ethical construct tied to various interpretations of international law.147 There is nothing in LOAC that conclusively states someone must be accountable for violations.148 Furthermore, the fact that AWS operate weapons uncontrolled by an operator does not inherently make it illegal. For example, anti-vehicle mines—not covered by the Ottawa Convention, of which the United States is not a signatory—are legal. This is the case, despite the fact that a human operator does not control whether or when an enemy or civilian

---

145. Even with UCAs, LOAC and IHL violations committed by their use are most often the consequence of an error by the human operator as opposed to a weakness in the technology, see The LAW OF ARMED CONFLICT, supra note 95, at 551.

146. See MIND THE GAP, supra note 93, at 18-19.

147. While Robert Sparrow’s Killer Robots is the penultimate article for arguing why AWS should be prohibited based on accountability from an ethical standpoint, Mind the Gap, a joint report between HRW and the International Human Rights Clinic (IHRC) at Harvard Law School builds off of Sparrow’s article and encapsulates the main legal issues against the use of LAWS based on accountability issues. The report describes what the necessary requirements are to assign responsibility to individuals and the reasons from various areas of the law why it is important to find one accountable for violations. Finally, the report goes through those who would be investigated for responsibility (i.e. military LAWS operators/commanders who would control the missions LAWS are placed on and private industry manufacturers/programmers who would construct and maintain LAWS) and how in certain circumstances, no one could be held accountable for LAWS violations, or how any punishment meted would be unsatisfactory to deter future violations or would not provide sufficient justice to the victims. These reasons provide the basis for an international prohibition on the technology. See generally Robert Sparrow’s Killer Robots, 24 J. APPLIED PHILOSOPHY 62 (2007); MIND THE GAP, supra note 90.

148. Thurnher, supra note 110, at 82.
vehicle sets off the mine. The United States recognizes that there is no obligation to require weapons themselves to abide by LOAC principles. Yet, it also recognizes that in a situation in which a person is using AWS to select and engage targets autonomously, “that person must refrain from using that weapon where it is expected to result in incidental harm that is excessive in relation to the concrete and direct military advantage expected to be gained,” or else that person will be held accountable for LOAC violations. This demonstrates that there are instruments available in order to hold persons accountable for LOAC violations by AWS.

A key step to holding personnel accountable is the creation of regulations and standards of care that can provide notice to personnel on the standard operating procedures (SOPs) for AWS so that such personnel know what actions committed by the AWS implicate personal responsibility. First, humans must design and program the AWS. These individuals would be responsible for designing and programming weapons systems to engage in actions that they know to be LOAC violations. If remote human supervisors are used for monitoring the AWS, these individuals could also be liable for violations by the AWS. If a remote supervisor knows that the AWS is about to engage an illegal target, and yet does nothing to impede such actions, they could be held accountable. Additionally, if the AWS does not engage an illegal target, but a remote supervisor overrides this decision, directing the AWS to engage such a target, the remote supervisor could be held liable for such a violation, if it was unreasonable. The DoD’s Uniform Code of Military Justice also offers outlets for punishing military personnel for such violations, such as dereliction of duty and even murder.

Accountability for the remote supervisor who is actively monitoring the AWS through a live feed would not be so different from the tactical commander who orders and specifies a mission for the AWS. In both situations, the supervisor and the commander would not actively be in the AWS’ decision loop. Command responsibility seemingly applies in

---

149. ARMIN KRISHNA, KILLER ROBOTS: LEGALITY AND ETHICALITY OF AUTONOMOUS WEAPONS 105 (Routledge 2013).
150. See LAW OF WAR MANUAL, supra note 85, at 330.
151. See id.
152. See Kastan, supra note 24, at 66.
153. See Schmitt & Thurnher, supra note 10, at 278.
154. See Kastan, supra note 24, at 78-79.
155. See id. at 79.
each case because both the supervisor and commander are expected to maintain operational control of the AWS as with any military equipment under their command. 156 Just as a programmer could be held liable for knowingly fielding AWS that is unable to distinguish targets on the battlefield, the commander could also be held liable if they allow such a system to operate. Moreover, if the commander only later learns of the faulty AWS operation, resulting in civilian deaths, and fails to investigate or hold those subordinates accountable, the commander again could be liable.157

The DoD, through Directive 3000.09, provides guidance on AWS commanders’ responsibilities by stating:

Persons who authorize the use of, direct the use of, or operate autonomous and semi-autonomous weapon systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement.158

Furthermore, customary international law, international tribunals, and AP I, Article 86(2) holds commanders accountable if they are actually aware that LOAC violations would occur by subordinates or materiel under their control, or even if they constructively should have been aware, but failed to take action.159

In certain respects, AWS could actually be a benefit in maintaining accountability for LOAC violations. AWS could be able to stream footage to remote supervisors, but also keep recordings onboard to ensure if there is a possible violation, there could be two copies to verify remote supervisors’ actions, as well as an additional method of verification to see if the remote supervisor’s feed was tampered with or edited.160 Therefore, while AWS seemingly create new challenges within international law, their future use could potentially promote adherence and accountability within LOAC.

156. See Toscano, supra note 21, at 236.
157. Schmitt & Thurnher, supra note 10, at 278.
158. See Directive 3000.09, supra note 3, at 3.
159. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, VOLUME I: RULES 558 (Cambridge Univ. Press 2009); See AP I, supra note 44, at Art. 51(4)(c).
160. See Toscano, supra note 21, at 239.
V. CONCLUSION/RECOMMENDATIONS

Simply because technology may allow for the successful development of AWS does not mean that international law will permit their unrestricted use. In this manner, AWS are no different from how international law applies to other weapons; it regulates their use under the principles of LOAC. It is clear, however, that AWS are not currently prohibited from being fielded by any provision or rule within international law. However, the legal use of AWS should be limited to ensure that they will reasonably abide by LOAC and IHL principles in international customary and treaty law.

Many of the limitations that should be implemented for compliance should be based on the reasonable confidence of commanders in the ability of the hardware and software of AWS technology to abide by LOAC in a multitude of reasonable situations. This confidence should be predicated on the reliability and predictability an AWS will have in certain missions, as seen with current defensive AWS such as Aegis. Reliability and predictability ought to be determined based on “strict operational constraints with respect to the task carried out, the targets attacked, the operational environment, the geographical space and time of operation, the scope to enable human oversight of the operation of the weapon system, and the human ability to deactivate it if need be.”161 This has been the case with both Aegis and Patriot, which has helped avert any strong call for their prohibition.

Furthermore, commanders and others within the chain of AWS design, maintenance, and operation should be culpable for the actions and potential LOAC violations committed by AWS. This accountability would ensure, at least partially, that the confidence of commanders would be balanced and not unreasonable. Establishing standards of design/maintenance/operation would aid in providing expectations for personnel, so that this balancing effort would not be an excessively difficult or time-intensive endeavor. Keeping legal advisors at hand in establishing these regulations, and within the decision process when they are carried out, would also be valuable. This would help demonstrate that AWS are similar to weapons already fielded, and may actually lessen the death and destruction in war, tempering calls for an international ban.

Additionally, taking part in meaningful discussions, through current ICRC and United Nations-led meetings regarding AWS, could aid in

161. See VIEWS OF THE INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) ON AUTONOMOUS WEAPON SYSTEM, supra note 20, at 3.
overcoming a prohibition. These bodies could also help to guide and establish limits in international treaty form, such as in the CCW, of what is actually considered AWS as well as limiting the autonomy allowed based on operational parameters of AWS.\footnote{162} Robust engagement and commonsense restrictions would help to ensure that these powerful weapons are developed and fielded in accordance with the internationally-recognized and established laws of war.

\footnote{162. The U.N. has already held several meetings since 2014, with the latest being April 2016 at the third informal meeting of CCW experts to discuss AWS in terms of four areas: definitions, human control, accountability, and weapons review. Meetings in 2017 and 2018 are believed to move to more formal meetings, exemplifying the movement to solidifying if there should be negotiations to adopt regulations on AWS in the CCW, or a full ban, see Chris Ford & Chris Jenks, \textit{The International Discussion Continues: 2016 CCW Experts Meeting on Lethal Autonomous Weapons}, \textit{JUST SECURITY} (Apr. 20 2016), \url{www.justsecurity.org/30682/2016-ccw-experts-meeting-laws/}.}