AUTONOMOUS WEAPON SYSTEM AND COMMAND RESPONSIBILITY

*Vivek Sehrawat**

Abstract

Autonomous Weapon Systems (AWS) are gradually becoming incorporated into warfare as technology advances and capabilities increase. The challenge of ensuring the responsibility for acts of an AWS poses some significant challenges. Under International Humanitarian Law (IHL) and international criminal law, individuals are criminally responsible for any war crimes they commit. It is unclear who can be held responsible for deaths and war crimes committed by AWS. This Article is focused on human-out-of-the loop weapons. This Article outlines the legal theory of command responsibility, which international criminal courts may apply to achieve responsibility. This Article examines the individual and state responsibility, and a test for determining command responsibility is conducted. Further, this Article discusses the intent and command responsibility, international criminal law framework for AWS, and the search for criminal culpability. Finally, this Article provides four solutions for command responsibility in relation to AWS.

INTRODUCTION

The legality of autonomous weapon systems (AWS) is an important issue under international law as technology advances, and machines acquire the capacity to operate without human control.[1] The advent of AWS creates new challenges that need to be addressed. AWS poses significant challenges to ensuring the responsibility for its acts. Individuals are criminally responsible for war crimes under International Humanitarian Law (IHL) and international criminal law.[2] Also, they can be held responsible under different modes of liability, such as for attempting, assisting, facilitating, aiding, abetting, planning, or instigating the commission of a war crime.[3] However, it is unclear who can be held responsible for deaths and war crimes committed by AWS. People demand responsibility and accountability.

AWS are gradually becoming incorporated into warfare with the advancement of technology and increased capabilities of sensors, analytical capabilities, and their integration in response to the increasing tempo of military operations.[4] Also, AWS are incorporated because of political pressures to protect combats, civilians, and property.[5] Automation in weapons systems will be a general feature across battlefield environments, and genuine autonomy in weapons will probably remain rare for the foreseeable future.[6]

Also, AWS are different from the remote-controlled weapon systems, like the Predator and Reaper drones that the United States (U.S.) has. In AWS, an onboard computer chooses the targets and makes decisions autonomously without a human in the loop.

---

* Vivek Sehrawat is an Assistant Professor of Law at BML Munjal University. He has extensive research and publication experience in legal issues relating to National Security, international humanitarian law, international law, and privacy law. Vivek conducted extensive research on drones during his SJD at University of Kansas. After finishing his SJD, he joined University of California, Davis as a Visiting Scholar. At Davis, he continued his work on drones as well as the legal implication of autonomous weapon systems. From that research, he authored this book. At Davis, he worked on the UN Human Rights in the field of cultural rights projects with the Special Rapporteur Karima Bennoune. He served on the editorial board of the UC Davis Business Law Journal during his LLM.

1. Vivek Sehrawat, *Autonomous weapon system: Law of armed conflict (LOAC) and other legal challenges*, 33 COMPUTER L. & SEC. REV.: THE INT'L J. OF TECH. L. AND PRAC. 38 (2016).
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*

The incremental evolution of AWS technologies should be recognized for the future to address the legal and ethical dilemmas; the U.S. should assume the foreseeability of AWS and build policies towards resolving these ethical dilemmas.[7] Prohibitory treaties are unworkable and ethically questionable because there are certain yet gradual development, deployment, and humanitarian advantages created by the precision of these systems.[8]

Scholars and researchers have taken a number of approaches to address the responsibility issues posed by AWS. Scholars such as Robert Sparrow has argued that no one will be responsible because it is not possible to describe any responsibility for the behavior of AWS to a human.[9] Other scholars, such as Peter Asaro, believe that AWS will eventually be responsible for their actions.[10] A number of other possible *loci* of responsibility for AWS war crimes are canvassed: the persons who designed or programmed the system, the commanding officer who ordered its use, and the machine itself. Punishing a machine for autonomous decisions is inappropriate and impractical.

According to Human Rights Watch, three human actors can be held responsible for the crimes committed by an AWS. These are commanders, programmers, and manufacturers.[11] However, opponents have identified several flaws with each of these potential candidates for responsibility.[12] Prosecuting three human actors individually and successfully is challenging because it is necessary to prove the intention or knowledge of AWS.[13] Also, several scholars offered rules or informal laws for designers and users of artificial agents to encourage a clear allocation of responsibility.[14] For example, Keith Miller initiated and led a collective effort to develop a set of rules for 'moral responsibility for computer artifacts.'[15] According to the rules, there is a shared responsibility for the designer, developer, and commander of the computer artifacts.[16] The rules indicate that these people will take

7. Kenneth Anderson & Matthew Waxman, *Law and Ethics for Robot Soldiers*, 2 (COLUM. PUB. L. RES. PAPER 12-313, 2012).

8. *Id.*

9. Robert Sparrow, *Killer Robot*, 24 J. OF APPLIED PHIL. 64, 66 (2007).

10. Ida Verkleij, Fully Autonomous Weapon Systems (2016) (unpublished Master's thesis, Tilburg University) (*available at* http://arno.uvt.nl/show.cgi?fid=141890).

11. *Id.*

12. Daniel Hammond, *Autonomous Weapons and the Problem of State Accountability,* 15 CHI. J. OF INT'L L. 652, 654 (2015).

13. Sehrawat, *supra* note 1.

14. Deborah G. Johnson & Merel Noorman, *Recommendations for Future Development of Artificial Agents*, TECH. AND SOC'Y, Jan. 2014, at 2.

15. *Id.*

16. *Id.*

responsibility for AWS when they consider the sociotechnical systems in which the artifact is embedded.[17]

Similarly, Robin Murphy and David Woods developed three laws of responsible robotics, intended as alternatives to Asimov's three rules from I-Robot.[18] According to Murphy and Woods' laws, robots should be designed to be responsive to humans.[19] For example, "A human may not deploy a robot without the human-robot work system meeting the highest legal and professional standards of safety and ethics."[20]

Also, few scholars considered holding a state accountable as feasible for crimes committed by AWS.[21] Indeed, hardly any scholars questioned the desirability in theory or feasibility in practice.[22] Yet, no scholar created a coherent definition of autonomy in weapon systems from a command responsibility perspective under IHL. This often results in the conflation of legal, ethical, policy, and political arguments.

AWS is divided into three categories based on human involvement in their actions:

- Human-in-the-Loop Weapons: AWS that can select targets and deliver force only with a human command;
- Human-on-the-Loop Weapons: AWS that can select targets and deliver force under the oversight of a human operator who can override the robots' actions; and
- Human-out-of-the-Loop Weapons: AWS that are capable of selecting targets and delivering force without any human input or interaction.[23]

Human-out-of-the-loop weapons are the primary concern; however, human-in-the-loop and human-on-the-loop weapons can also raise concern.[24] Human-out-of-loop weapons are more dangerous because human decision making is completely removed from the process.[25]

17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.*
21. Hammond, *supra* note 12.
22. *Id.*
23. *See generally* HUMAN RIGHTS WATCH & INT'L HUMAN RIGHTS CLINIC, HARVARD LAW SCHOOL, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS (2012).
24. Amos N Guiora, *Accountability and Decision Making in Autonomous Warfare: Who is Responsible*?, 4-2017 UTAH L. R. 393, 397 (2017).
25. *Id.*

Human decision making reflects consideration, deliberation, reflection, and doubt.[26] This Article is focused on human-out-of-the-loop weapons.

This Article assumes that AWS are not illegal weapons, and they may be used under certain circumstances. Some scholars believe that AWS are illegal under existing law. For example, their use cannot meet the requirements of international human rights and IHL principles of distinction and proportionality during the armed conflict.[27]

This Article outlines the legal theory of command responsibility, which can be applied by international criminal courts. This Article discusses the origins of command responsibility and responsibility concerns with AWS. It examines the individual and state responsibility and conducts a test for the determination of command responsibility. Further, this Article discusses the intent and command responsibility, the international criminal law framework for AWS, and the search for criminal culpability. Finally, this Article provides four solutions for the command responsibility in relation to AWS. In this Article term "accountability" and "responsibility" are used interchangeably.

I. DOCTRINE OF COMMAND RESPONSIBILITY

Discussion of command responsibility doctrine is important for a better understanding of this Article. The doctrine of command responsibility includes two concepts: (1) direct command responsibility: the commander can be held directly responsible for the order and (2) indirect command responsibility: the commander can be held responsible for the acts of his subordinates.[28] The second concept is based on the commander's failure to act when under a duty.

A. *Elements of Command Responsibility*

There are three elements of command responsibility:

(i) the existence of superior-subordinate relationships characterized by effective control over subordinates;

(ii) knowledge or constructive knowledge by the superior that his subordinates are about to commit or have committed genocide, crimes against humanity or war crimes; and

26. For a fascinating, important, and in-depth discussion of this issue *see* DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011).

27. CHRISTOF HEYNS, INT'L COMM. OF THE RED CROSS, AUTONOMOUS WEAPON SYSTEMS: TECHNICAL, MILITARY, LEGAL AND HUMANITARIAN ASPECTS 45 (Mar. 26–28, 2014).

28. Verkleij, *supra* note 10.

(iii) failure to adopt reasonable and necessary measures to prevent, punish or report the offenses.[29]

B. *The Origins of Command Responsibility*

This section discusses the historical background of the command responsibility in two sections, i.e., pre-World War II and post-World War II.

1. Post-World War II

The concept of command responsibility originated centuries ago. In around 500 BC, Sun Tzu wrote about the duty of commanders in *Ping Fa* - "the Art of War" to ensure subordinates conduct in armed conflict.[30] In 1439, Charles VII of Orleans promulgated an ordinance, requiring each captain or lieutenant will be held responsible for the abuses, ills, and offenses committed by members of his company.[31] The captain will be held responsible if the offender escapes and evades punishment because of his negligence or otherwise.[32] In 1474, the first international recognition of commanders' obligations to act lawfully occurred during the trial of Peter von Hagenbach by an ad hoc tribunal in the Holy Roman Empire.[33] Von Hagenbach was convicted of murder, rape, and other crimes which he should have prevented as a knight.[34] However, the Tribunal did not explicitly rely on a doctrine of command responsibility.[35] In the seventeenth century, Hugo Grotius wrote, "A community or its rulers may be held responsible for the crime of a subject if they knew of it and did not prevent it when they could and should prevent it."[36]

In 1779, the British Lieutenant Governor of Quebec, Henry Hamilton, was captured and tried for depredations committed by American Indians allied with the British during the American Revolution.[37] "It is noteworthy that the language of the indictment held that the acts of the Indians were the acts of Hamilton. He was considered personally liable

29. NICHOLAS TSAGOURIAS & ALASDAIR MORRISON, COMMAND RESPONSIBILITY IN INTERNATIONAL HUMANITARIAN LAW, CASES, MATERIALS AND COMMENTARY 337–67 (2018).

30. EUGENIA LEVINE, GLOBAL POL'Y FORUM, COMMAND RESPONSIBILITY: THE MENS REA REQUIREMENT (Feb. 2005).

31. GARY SOLIS, LAW OF ARMED CONFLICT: INT'L HUMANITARIAN L. IN WAR 382 (2010).

32. *Id.*

33. LEVINE, *supra* note 30.

34. *Id.*

35. *Id.*

36. SOLIS, *supra* note 31.

37. *Id.*

for the acts of subordinates."[38] The notion of command responsibility is controversial in consolidating the customary international law rule.[39]

2. Post-World War II Developments Concerning the Mens Rea of Command Responsibility

The doctrine of command responsibility linked to the criminal responsibility and its jurisprudence is developed after World War II.[40] The doctrine of command responsibility was first utilized formally after the end of World War II in war crime prosecutions.[41] Command responsibility has ancestries in the IHL principle of responsible command, under which commanders have to ensure that their subordinates respect IHL.[42] Under the command responsibility, the commander becomes criminally labile for the failure to prevent or punish offenses of the subordinates.[43] Therefore, Command responsibility is a powerful tool for enforcing compliance with IHL.[44] Command responsibility was left almost untouched for forty years after World War II, and later a number of issues were clarified and introduced in the Statutes of the International Criminal ad hoc Tribunals.[45]

Also, in modern times, the issue of responsibility is important. In the military context, commanders and soldiers are subject to disciplinary sanctions and courts-martial for mundane or serious offenses.[46] The essence of command responsibility is that commanders may suffer career-ending consequences.[47] A system without command responsibility is directly contrasted to the IHL principles.[48] Decision making and responsibility are directly related.[49] States authorize "Kill or not kill" decisions and standards of responsibility are not inherent or integral in authorizing the new Wild West.[50]

---

38. *Id.*
39. Micaela Frulli, *Exploring the Applicability of Command Responsibility to Private Military Contractors*, 15 J. OF CONFLICT & SEC. L. 435, 437 (2010).
40. *Id.*
41. TSAGOURIAS & MORRISON, *supra* note 29.
42. *Id.*
43. *Id.*
44. *Id.*
45. Frulli, *supra* note 39.
46. Guiora, *supra* note 24, at 398.
47. *Id.*
48. *Id.* at 397.
49. *Id.* at 398.
50. *Id.*

Command Responsibility Under the Rome Statute of the ICC Article 25(3) provides:

> A person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court if that person:
>
> (b) Orders solicits or induces the commission of such a crime, which in fact occurs or is attempted.[51]

IHL Customary Rule 153 says that:

> commanders and other superiors are criminally responsible for war crimes committed by their subordinates if they knew, or had reason to know, that the subordinates were about to commit or were committing such crimes and did not take all necessary and reasonable measures in their power to prevent their commission, or if such crimes had been committed, to punish the persons responsible.[52]

State practice establishes the applicability of command responsibility rule as a norm of customary international law in both international and non-international armed conflicts.[53] Individual criminal responsibility for war crimes and crimes against humanity is important and continually established by the contemporary international criminal tribunals and courts, such as the International Criminal Tribunal for former Yugoslavia, the International Criminal Tribunal for Rwanda, the Special Court for Sierra Leone, and the International Criminal Court.[54] In the twenty-first century, with the advancement of technology, imposing criminal liability is challenging for an individual for the act of a machine.

II. RESPONSIBILITY CONCERNS WITH AWS

The delegation of human decision-making responsibilities to an AWS is the moral and legal issue because they are designed to take human lives.[55] The operational constraints are critical from an ethical point of

---

51. INT'L COMM. OF THE RED CROSS, IHL DATABASE, PRACTICE RELATING TO RULE 152, COMMAND RESP. FOR ORDERS TO COMMIT WAR CRIMES.

52. INT'L COMM. OF THE RED CROSS, IHL DATABASE, RULE 153, COMMAND RESP. FOR FAILURE TO PREVENT, REPRESS OR REPORT WAR CRIMES.

53. *Id.*

54. Jack Beard, *Autonomous Weapons and Human Responsibilities*, 45 GEO. J. OF INT'L L. 617, 642 (2014).

55. Peter Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making*, 94 INT'L REV. OF THE RED CROSS, 687, 695 (2013).

view.[56] There are some grave and core concerns with the use of AWS for targeting humans as an AWS does not have human agency, intent, moral responsibility, and human dignity.[57]

Ceding the use of force and life-and-death decisions to the machines instead of humans raises fundamental ethical questions. According to ICRC, responsibility and accountability for decisions to use force cannot be transferred to a machine or a computer program.[58] These are human responsibilities—both legal and ethical—which require human agency in the decision-making process.[59] Therefore, a closely related ethical concern raised by AWS is the risk of erosion—or diffusion—responsibility and accountability for these decisions.[60]

Matthias refers to this issue as 'the responsibility gap.'[61] AWS can be programmed to learn as they operate, and because of this learning, the fear is that no humans—even the programmers of the agents—will not be able to understand the decision making of artificial agents.[62] Hence, no human can fairly be held responsible for the action of artificial agents.[63] However, there are several possible scenarios for the responsibility of AWS war crimes; designer or programmer, the commanding officer who ordered its use, and the machine itself.[64] Also, some scholars identified States to be held responsible for filling the responsibility gap.

The responsibility concern remains a challenge for the legal scholar, and none of these are satisfactory. Responsibility is a necessary condition under the principle of IHL that someone can be held responsible for war crimes.[65]

III. RESPONSIBILITY FOR AWS

The responsibility for AWS can be divided into two categories: individual responsibility and state responsibility. If AWS possesses no agency or legal personality of their own, then the individual(s) can be held criminally responsible for their role as operators, commanding officers, programmers, engineers, technicians, or other relevant

56. Neil Davison, *Autonomous Weapon Systems: An Ethical Basis for Human Control?*, HUMANITARIAN L. & POL'Y (Apr. 3, 2018), https://blogs.icrc.org/law-and-policy/2018/04/03/autonomous-weapon-systems-ethical-basis-human-control/.

57. *Id.*

58. INT'L COMM. OF THE RED CROSS, ETHICS AND AUTONOMOUS WEAPON SYSTEMS: AN ETHICAL BASIS FOR HUMAN CONTROL? 2 (Apr. 3, 2018).

59. *Id.*

60. *Id.*

61. Johnson & Noorman, *supra* note 14.

62. *Id.*

63. *Id.*

64. Sparrow, *supra* note 9.

65. *Id.*

functions.[66] If the deployment of an AWS seriously violets IHL, then the individuals can be criminally prosecuted for war crimes, crimes against humanity, or genocide.[67] Also, a state can be held responsible for the development and deployment of AWS. The following sections discuss the individual responsibility and state responsibility.

A. *Individual Responsibility*

There is consensus among delegations of the Group of Governmental Experts that humans should be held legally responsible for the autonomous decision making powers in targeting, and AWS cannot be considered criminally responsible.[68] Ultimately, humans should be held criminally responsible because they are involved in the deployment of AWS.[69] This falls under the cardinal principles of criminal law that human action is a prerequisite for criminal responsibility. Also, under international criminal law, war crimes can only be committed by individuals and not by robots.[70]

Additionally, the supervisor could be held liable if the AWS engage in an illegal and unreasonable target because a supervisor is involved in the deployment of the AWS.[71] Also, the Department of Defense's Uniform Code of Military Justice provides punishment for violations by military personnel, such as dereliction of duty and murder.[72] Accountability for the supervisor who actively monitors the AWS through a live feed would be similar to the tactical commander who orders and specifies a mission for the AWS.[73] In both scenarios, the supervisor and the commander would not actively be in the AWS's decision loop.[74]

Commander is expected to maintain operational control of the AWS as with any military equipment under their command.[75] A programmer could be held liable for knowingly deploying an AWS that is unable to

66. Nikolas Sturchler & Michael Siegrist, *A "Compliance-Based" Approach to Autonomous Weapon Systems,* EJIL:TALK! (Dec. 1, 2017), https://www.ejiltalk.org/a-compliance-based-approach-to-autonomous-weapon-systems/.

67. *Id.*

68. Marta Bo, *Who is Criminally Responsible for the Commission of War Crimes When Lethal Autonomous Weapon Systems are Deployed in Armed Conflicts?*, THE GRADUATE INSTITUTE GENEVA (Sept. 21, 2018), https://graduateinstitute.ch/communications/news/who-criminally-responsible-commission-war-crimes-when-lethal-autonomous-weapon.

69. *Id.*

70. *Id.*

71. Michael Press, *Of Robots and Rules: Autonomous Weapon Systems in the Law of Armed Conflict*, 48 GEO. J. OF INT'L L. 1337, 1363 (2018).

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.* at 1364.

satisfy the principle of distinction during war; similarly, the commander could be held liable if they allow such a system to operate.[76] Also, the commander can be held liable if the commander later learns of the faulty AWS operation, causing civilian deaths, and fails to investigate or hold subordinates accountable.[77]

The first element of command responsibility needs to be satisfied, i.e., the existence of a superior-subordinate relationship. The challenge here is who is superior and who is subordinate. If the commander is superior, then AWS becomes subordinate. "The scenario where any such person would say 'the machine did it' is easy to imagine."[78] According to this element, AWS needs to be punished, but that is not possible. Another scenario could be if the programmer is subordinate, then the commander could be punished.

Then there is the second element, i.e., knowledge or constructive knowledge by the superior that his subordinates are about to commit or have committed genocide, crimes against humanity, or war crimes. In this scenario, it will be challenging to justify that the commander knew about the AWS committing war crimes. In another scenario, when a chip goes off or if a problem occurs with the software, then it will be challenging for a programmer or manufacturer to determine the fault, which might result in war crimes.

The third element is the failure to adopt reasonable and necessary measures to prevent, punish, or report the offenses. It will not be possible to punish AWS. The reasonable and necessary measure to prevent offenses is to ban the AWS or to punish the developer of AWS.

The concept of responsibility for the actions of AWS is challenging and unclear.[79] Implementing robust responsibility standards and criteria is uncertain because the decision making is largely removed from the commanders.[80] Therefore, the machine that took the unpredictable decision would be the argument because computers act randomly, and they operate in complex environments.[81] The interactions between the system and the surroundings cannot be foreseen.[82] If responsibility is assigned by law in theory, in practice, those who activate AWS may find sympathy from judges and others who have to assess their conduct.[83] The danger of an accountability gap remains in theory and practice.[84]

---

76. *Id.*
77. *Id.*
78. HEYNS, *supra* note 27, at 46.
79. *Id.*
80. Guiora, *supra* note 24, at 419.
81. HEYNS, *supra* note 27, at 46.
82. *Id.*
83. *Id.*
84. *Id.*

Professor Michael Schmitt's views, accountability contentions "muddled" the debate about AWS.[85] He observes, it is not difficult to map out the accountability allocation: "Clearly, any commander who decides to launch AWS into a particular environment is, as with any other weapon systems, accountable under international criminal law for that decision. Nor will developers escape accountability if they design systems, autonomous or not, meant to conduct operations that are not IHL compliant."[86]

Similarly, Professor Armin Krishnan said that the "legal problems with regard to accountability might be far smaller than some critics of military robots believe."[87] He views that if "the robot does not operate within the boundaries of its specified parameters, it is the manufacturer's fault."[88] Also, if the AWS is "used in circumstances that make its use illegal, then it is the commander's fault."[89]

Case in point: An IDF battalion commander was given an order to detain three suspected terrorists in Nablus.[90] When approaching the city, the commander received an urgent update from his intelligence officer that while spotters had located the suspected terrorists, they were surrounded by school-age children.[91] The commander had, according to his analysis, three options: (1) cancel the mission; (2) proceed with the mission, regardless of the consequences to the children; or (3) engage in "cat and mouse" with the terrorists.[92] The commander decided to cancel the mission.[93] He reasoned that the costs of collateral damage did not outweigh the benefits accrued from arresting the three, and the mission could be achieved at a later date.[94]

This example highlights both the issue of responsibility and the consequence of minimizing and importance of human input in decision making.[95] Responsibility is the essence of command.[96] The command structure is dependent on the proper delegation of responsibility and accountability.[97] Combats and commanders depend on a command

85. Charles Dunlap Jr., *Accountability and Autonomous Weapons: Much Ado About Nothing?*, 30 TEMPLE INT'L & COMP. L.J. 63, 68 (2016).

86. *Id.* at 69.

87. ARMIN KRISHNAN, KILLER ROBOTS: LEGALITY AND ETHICALITY OF AUTONOMOUS WEAPONS (2009).

88. *Id.*

89. *Id.*

90. Guiora, *supra* note 24, at 420.

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

structure that ensures military discipline, clear lines of command, a confirmation of systemic and institutionalized principles of accountability and responsibility.[98]

Additionally, human actors can be held responsible for direct and indirect command responsibility. In direct responsibility, the commander can be held responsible for ordering his subordinates to carry out unlawful conduct.[99] In indirect responsibility, the commander can be held liable for a subordinate's unlawful conduct and failure to act. However, there should be standard operating procedures for AWS to hold personnel accountable, which can be achieved by creating regulations and standards of care. This will help personnel know what actions committed by the AWS implicate personal responsibility.[100]

Also, it can be under the perpetrator responsible for failing to act. Under the Geneva Conventions of 1949 for repressing grave breaches targets persons who have committed or ordered the commission of such breaches.[101] Commanders can be held criminally liable for not acting and allowing a grave breach.[102] For example, failing to act when killing someone by withholding food, proper care, and the grave breach of depriving a prisoner of war of the right to a fair trial.[103]

Article 86 (1) Additional Protocol I of 1977 is more explicit:

> The High Contracting Parties and the Parties to the conflict shall repress grave breaches and take measures necessary to suppress all other breaches of the Conventions or of this Protocol, which result from a failure to act when under a duty to do so.[104]

Article 85 of Additional Protocol I refers to grave breaches that are generally committed by a failure to act, such as the unjustified delay in repatriating prisoners of war or civilians.[105] Existing mechanisms for legal accountability are ill-suited and inadequate to address the unlawful harms of AWS might cause.[106] Individual responsibility is a challenging concept because the human element is absent from the decision making in AWS, and also there are multiple individuals involved in the use of

98. *Id.*

99. INT'L COMM. OF THE RED CROSS, ADVISORY SERVICE ON INTERNATIONAL HUMANITARIAN LAW, COMMAND RESPONSIBILITY AND FAILURE TO ACT (Apr. 2014).

100. Press, *supra* note 71, at 1363.

101. INT'L COMM. OF THE RED CROSS, *supra* note 99.

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. HUMAN RIGHTS WATCH, MIND THE GAP, THE LACK OF ACCOUNTABILITY FOR KILLER ROBOTS (Apr. 9, 2015).

AWS. States should incorporate punishment for the commander, designer, and programmer for the acts of AWS.

1. State Responsibility

Under the State responsibility, a State could be held liable for violations of IHL resulting from the use of an AWS. Also, under international law governing the responsibility of States, they would be held responsible for internationally wrongful acts, such as violations of IHL committed by their armed forces for using an AWS.[107] A State will also be responsible if it deploys an AWS without adequately testing and reviewing.[108]

The UN Group of Governmental Experts overlay the *Tallinn Manual's* articulation of state responsibility with AWS.[109] If the *Tallinn Manual's* criteria for state responsibility for cyber warfare were co-opted to apply to AWS, then states would be responsible for the acts committed by AWS under two conditions: (1) When the act of an AWS is attributable to the state under international law; or (2) When the AWS act constitutes a breach of an international legal obligation applicable to the States.[110]

For example, if an AWS malfunctions resulting in harm or killing of innocent civilians in a foreign combat environment, i.e., a breach of an international legal obligation, then (1) the act would be attributed to the state employing the technology and (2) the state would be held accountable for breaching an international legal obligation to protect the innocent civilians.[111]

States are responsible for wrongful acts under international law that are attributable to AWS, but this does not extend to criminal responsibility.[112] States can be held accountable for human rights violations and can be required to cease unlawful actions and pay compensation.[113] However, this does not frequently happen for IHL violations.[114] The role of States for accountability could play a potentially important role in deciding which weapons to acquire, and the obligation of weapons review.[115]

---

107. NEIL DAVISON, INT'L COMM. OF THE RED CROSS, A LEGAL PERSPECTIVE: AUTONOMOUS WEAPON SYSTEMS UNDER INTERNATIONAL HUMANITARIAN LAW 16 (2016).

108. *Id.*

109. Jessica Malekos Smith, *Imagining a Killer Robot's First Words: Engineering State-in-the-Loop Legal Responsibility for Fully Autonomous Weapons Systems*, HARV. KENNEDY SCH. REV. (July 12, 2018), https://ksr.hkspublications.org/2018/07/12/imagining-a-killer-robots-first-words-engineering-state-in-the-loop-legal-responsibility-for-fully-autonomous-weapons-systems/.

110. *Id.*

111. *Id.*

112. HEYNS, *supra* note 27, at 46.

113. *Id.*

114. *Id.*

115. *Id.*

UN Charter governs the recourse of the threat or use of force by States.[116] States have a duty to control or supervise the development, employment of AWS, and usefully define and exert.[117] For example, it is sufficient to rely on superior programming and strict reliability testing to make an AWS predictably compliant with IHL for its intended operational parameters.[118] Thus, it would be permissible to restrict human involvement to the proper activation of such an AWS.

As Professor Michael Schmitt points out, "States can be held accountable under the laws of State responsibility armed forces use AWS in an unlawful manner."[119] Ultimately, the support for employing AWS must be conditioned on their potential to mitigate suffering in war and the international community's ability to abide by State responsibility.[120]

IV. INTENT AND COMMAND RESPONSIBILITY

Intent is an important aspect of proving criminal liability under command responsibility and international law. A commander cannot be held criminally responsible without proving the intention to commit a crime. Some scholars believe AWS would lack certain human characteristics, such as judgment, compassion, and intentionality.[121] AWS has the potential to commit criminal and unlawful acts that would constitute a crime if done with intent, for which no one could be held responsible.[122] An AWS itself could not be responsible for criminal acts that it might commit because it would lack intentionality.[123] For example, an AWS would have the potential to direct attacks against civilians, kill or wound a surrendering combatant, and launch a disproportionate attack; they are elements of war crimes under the Rome Statute of the ICC.[124] By contrast, AWS could not have the mental state required to make these crimes; because they would not have moral agency, they would lack the independent intentionality that must accompany the commission of criminal acts to establish criminal liability.[125]

However, the UK defines an automated system as ". . . programmed to logically follow a pre-defined set of rules with predictable outcomes," whereas an autonomous system is ". . . capable of understanding higher-level intent and direction."[126] An AWS would be capable of

116. Sturchler & Siegrist, *supra* note 66.
117. *Id.*
118. *Id.*
119. Dunlap Jr., *supra* note 85, at 69.
120. Smith, *supra* note 109.
121. HUMAN RIGHTS WATCH, *supra* note 106.
122. *Id.*
123. *Id.*
124. *Id.*
125. *Id.*
126. *See* HEYNS, *supra* note 27, at 18.

understanding, perceiving its environment, and deciding a course of action from a number of alternatives without depending on human oversight and control.[127] According to the UK, AWS's activities would be predictable.[128]

Human commanders or operators could be assigned direct responsibility for the crimes of an AWS in exceptional circumstances. For example, if a programmer intentionally programs an AWS to commit war crimes, he or she could be held accountable.[129] Even if the programming occurred in peacetime, the programmer could be held liable for committing or assisting a war crime if the AWS carried out the activities during the armed conflict.[130] Therefore, the programmer or operator could be held accountable if they acted with criminal intent in programming or at least has knowledge of the AWS's criminal act, and the intent has to be proven. However, there are significant challenges in proving intention and holding anyone responsible for an AWS's conduct under international criminal law.[131] The lack of human control and unpredictability of AWS makes it challenging to find individuals involved in the programming and deployment criminally liable for war crimes because commanders and programmers may not have the knowledge or intent required for such acts.[132] This leaves a command responsibility gap.

Command responsibility does not require the commander's direct criminal responsibility for crimes committed by his subordinates, but for culpable failure to prevent, suppress or repress crimes committed by persons, i.e., not machines, under his or her command and control.[133] Also, a commander's failure to control AWS operating under his or her command may constitute a direct violation of the duties of precaution, distinction, proportionality, or any other obligation imposed by IHL.[134] The functions of human soldiers are increasingly "delegated" to AWS. It may become appropriate *de lege ferenda* to extend the commander's supervisory duty, *mutatis mutandis,* and by analogy, also to AWS operating under his direct command and control.[135]

Direct command responsibility is explained in Article 7 (1) of the ICTY statute and Article 6 (1) of the ICTR:

127. *Id.*
128. *Id.*
129. *Id.* at 23.
130. *Id.*
131. *Id.*
132. *Id.*
133. Sturchler & Siegrist, *supra* note 66.
134. *Id.*
135. *Id.*

> A person who planned, instigated, ordered, committed or otherwise aided and abetted in the planning, preparation or execution of a crime referred to in articles 2 to 5 of the present Statute, shall be individually responsible for the crime.[136]

Therefore, direct command responsibility can be established for the positive acts of the commander.[137] In AWS, "ordering" is the most applicable action of the commander.[138] According to the *actus reus* (an illegal act) of "ordering" a crime requires that the commander should order to subordinate to commit an offense.[139] Such a commander can be *de jure*, *de facto*, or reasonably implied.[140] It is sufficient if there is some proof of authority on the part of the accused.[141] To establish the *mens rea* requirement (intent) for "ordering" a crime, it must be proven that the commander ordered an act with the awareness of the substantial likelihood that a crime will be committed in the execution of the order.[142] The *mens rea* of the accused does not need to be explicit but may be inferred from the circumstances.[143]

The human commanders or operators could not be held directly responsible for the wrongful acts of an AWS without proving intent. Also, imposing criminal punishment on the programmer or manufacturer will be challenging and unreasonable for the wrongful acts of AWS.[144] Therefore, it would be challenging to identify a specific individual with the intention to commit crimes in the complex development and manufacturing chain.

V. THE INTERNATIONAL CRIMINAL LAW FRAMEWORK

Command responsibility doctrine is a complex form of criminal responsibility. IHL is the most relevant body of international law governing the development and employment of AWS in armed conflicts.[145] Also, there are other branches of international law, such as human rights law, impose limits on the use of force in armed conflicts, and international criminal law governs individual criminal responsibility for violations.[146] The principle of individual criminal responsibility is one

136. Verkleij, *supra* note 10, at 19.
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.* at 20.
141. *Id.*
142. *Id.*
143. *Id.*
144. HUMAN RIGHTS WATCH, *supra* note 106.
145. Sturchler & Siegrist, *supra* note 66.
146. *Id.*

of the core principles of IHL for war crimes.[147] Punishing individuals for war crimes are significant in the enforcement of IHL.[148] The provisions of international law can be enforced by punishing individuals who commit war crimes because crimes are committed by humans, not by abstract entities.[149]

A. *AWS and the Search for Criminal Culpability*

There is the possibility if once engaged in the battlefield, AWS will target people and objects in violation of IHL rules on the methods of warfare because there is no human control involved in AWS's decision making. Therefore, there is a need to search the criminal culpable for the deployment of AWS. If AWS cannot be prosecuted because it is a machine for the crimes, this possibility offends not only the rule of law but also the more visceral human desire to find an individual culpable.[150]

In several domestic legal systems, civil lawsuits can be filled to hold individuals and companies responsible for the failure of machines.[151] Consumers in various countries, particularly the U.S., are protected under national product liability and safety laws that allow them to bring civil lawsuits against corporations for harm caused by manufactured or sold goods.[152] These lawsuits are usually based on various types of negligence, including manufacturing and design defects, failure to take proper care, avoid foreseeable risks, failure to warn, or provide reasonable instructions.[153] Scholars also suggested similar civil lawsuits as an option for incentivizing AWS manufacturers to produce harmless weapons.[154] For example, in the domestic system, Nevada has passed legislation imposing criminal liability as well as civil liability in driverless cars.[155] Driverless cars may not technically be 'fully' autonomous, but they are *de facto* similar because a driver's capability to intervene atrophies over time to the point of ineffectiveness.[156]

However, Human Rights Watch claimed that individual civil damages-by victims of illicit use of an AWS could not "fill the gap" they perceive to exist in the criminal law.[157] Their discussion mainly centers

147. Bo, *supra* note 68.
148. *Id.*
149. Beard, *supra* note 54, at 642.
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. Dunlap Jr., *supra* note 85, at 73.
156. *Id.*
157. *Id.*

on the complexity of the U.S. tort liability litigation generally, rather than weapons' law or the law of war.[158]

In *United States v. Kick*, the all-civilian Court of Military Appeals explained the necessity to criminalize behavior that breached the relatively low standard of simple negligence in the military.[159]

> There is a special need in the military to make the killing of another as a result of simple negligence a criminal act. This is because of the extensive use, handling, and operation in the course of official duties of such dangerous instruments as weapons, explosives, aircraft, vehicles, and the like. The danger to others from careless acts is so great that society demands protection.[160]

This illustrates the existing U.S. military law anticipates and recognizes the dangerous potential of weapons and imposes accountability even when "intentionality" is absent; therefore, Human Rights Watch wrongly thinks that intent must be present to impose criminal liability."[161] Indeed, this is just a sampling of the myriad of ways that, contrary to what Mind the Gap implies, any competent prosecutor could successfully pursue accountably when an AWS is employed.[162]

Additionally, under the U.S. Uniform Code of Military Justice Article 119 of manslaughter, criminalizes behavior where the accused "who, without an intent to kill or inflict great bodily harm" yet "unlawfully kills a human being . . . by culpable negligence."[163] "Therefore, involuntary manslaughter may be established by "a negligent act or omission which, when viewed in the light of human experience, might foreseeably result in the death of another, even though death would not necessarily be a natural and probable consequence of the act or omission."[164] It is possible to impose criminal liability on anyone involved in the culpably negligent use of an AWS.[165]

Also, the ICRC states that acting willfully includes acting with "wrongful intent" or "recklessness," which it describes as "the attitude of an agent who, without being certain of a particular result, accepts the possibility of it happening."[166] The ICRC distinguishes this from "ordinary negligence or lack of foresight," which occurs "when a man

158. *Id.*
159. *Id.* at 72.
160. *Id.*
161. *Id.*
162. *Id.* at 71.
163. MANUAL FOR COURTS-MARTIAL, United States, pt. IV ¶ 44 art. 119(b) (2012).
164. MANUAL FOR COURTS-MARTIAL, United States, pt. IV ¶ 44 art. 119(c)(2)(a)(i) (2012).
165. Dunlap Jr., *supra* note 85, at 72.
166. Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 UNIV. OF PA. L. R. 1347, 1377 (2016).

acts without having his mind on the act or its consequences (although failing to take necessary precautions, particularly failing to seek precise information, constitutes culpable negligence punishable at least by disciplinary sanctions)."[167]

At present, there is little sense in attempting to hold AWS liable.[168] Artificial intelligence has not advanced to a point where a robotic system could be said to act intentionally or recklessly.[169] If a violation of IHL is not a war crime absent some willful action, AWS are currently incapable of committing war crimes.[170] Additionally, traditional justifications for individual liability in criminal law—deterrence, retribution, restoration, incapacitation, and rehabilitation—do not map well from human beings to robots.[171] There is a need for more to find the fine line between appropriate risk mitigation and respect for personal culpability to establish criminal liability.

B. *Solutions*

The advent of AWS creates new challenges that need to be addressed. This section provides a different possible solution for AWS, keeping the doctrine of command responsibility in view. There is a need for a new legal framework for the AWS. This section presents the four possible solutions for the legal framework of AWS.

1. Existing Legal Framework

Some scholars argue that, while specific convention-based prohibitions may be lacking, AWS must, like all weapons, be used in compliance with applicable customary international law as reflected in the IHL framework.[172] Also, in the existing legal framework for command responsibility laws from international criminal tribunals, international criminal law and ICC statute of Rome can be applied. States and individuals can thus be held responsible for violations of IHL obligations involving the use of any weapon, depending on the facts of a particular case.[173]

However, the problem with these existing legal frames is that they are not designed to deal with modern technologies like AWS, where the human element is missing from decision making. It will be feasible to have new sets of laws that specifically govern the modern weapons of warfare, such as AWS.

---

167. *Id.*
168. *Id.*
169. *Id.*
170. *Id.*
171. *Id.*
172. Beard, *supra* note 54, at 642.
173. *Id.*

2. Banning AWS

Another possibility is that certain weapons may be classified as illegitimate under the IHL framework.[174] In the latter case, states are prohibited from employing such weapons under any circumstances because they are illegal per se.[175] However, as mentioned above, this Article is not about the legality of AWS and banning AWS. This is about providing a solution to the issue of command responsibility.

3. Autonomous Defense Systems

AWS can be developed just for defense purposes and banning all offensive AWS. For example, Iron Domes are autonomous as they can identify, track, and engage targets without human interference.[176] Iron Domes are intelligent, i.e., they can discriminate between projectiles that pose significant threats and projectiles that will ultimately fall in unpopulated areas and "strictly defensive," i.e., the system is utilized in a way that causes no immediate offensive advantage to its user and does not directly harm enemy combatants or enemy civilians.[177]

After 2011, the Israel Defense Force has used the Iron Dome system to shoot down over 1,700 unguided rockets and mortar shells launched by militants in Lebanon, Syria, and the Gaza Strip against Israeli communities.[178] An Iron Dome battery can also engage aircraft, drones, large artillery shells, and possibly even cruise and ballistic missiles.[179]

Another example, according to NBC News, South Korea installed stationary robots, developed by Samsung Techwin and Korea University.[180] The Samsung SGR-1 patrols the border between North and South Korea called the Demilitarized Zone.[181] Assistant Professor Heather Roff at the University of Denver said the SGR-1 was initially built with the capability to detect, target, and shoot intruders from two miles away.[182] She said, "In that sense, it's a really sophisticated landmine, it can sense a certain thing and can automatically fire."[183] But

---

174. *Id.*

175. *Id.*

176. Daphne Richemond-Barak & Ayal Feinberg, *The Irony of the Dome: Intelligent Defense Systems, Law, and Security*, 7 HARV. NAT'L SEC'Y J. 469, 494 (2016).

177. *Id.*

178. Sebastien Roblin, *This is Iron Dome (Israel's Rocket Crusher): Everything You Need to Know*, NATIONAL INTEREST (May 5, 2019), https://nationalinterest.org/blog/buzz/iron-dome-israels-rocket-crusher-everything-you-need-know-56057.

179. *Id.*

180. Guia Marie Del Prado, *These Weapons Can Find a Target all by Themselves-and Researchers are Terrified*, BUS. INSIDER (July 30, 2015), https://www.businessinsider.com/which-artificially-intelligent-semi-autonomous-weapons-exist-2015-7?IR=T.

181. *Id.*

182. *Id.*

183. *Id.*

Peter Asaro, the co-founder of the International Committee for Robot Arms Control, told NBC News that South Korea received "a lot of bad press about having autonomous killer robots on their border."[184] That is the reason now the SGR-1 can only detect and target but requires a human operator to approve the kill shot.[185] It is converted into semi-autonomous.

Another usage could be undertaking sustained surveillance, marking targets, gathering intelligence, deterring adversaries, and carrying out strikes in hostile territory, with the guiding hand of a human operator.[186] But the development of semi-autonomous weapons are secretive, and it's unclear what part humans play in choosing and firing on targets.[187]

Using Iron Dome or semi-autonomous systems might provide a solution for the command responsibility because they are used for defensive purposes and, therefore, minimizes the casualties. Also, they have a human element; therefore, it is feasible to hold the commander liable.

4. Standard Operating Procedures for AWS

AWS are a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system.[188] Therefore, it will be unfair to apply laws of other weapon systems that have a human element, and war crimes cannot be measured with the existing laws and standards. It creates a situation to look for different laws and regulations for 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 for AWS so that such personnel knows what actions committed by the AWS implicate personal responsibility.[189] A key adjustment that must be made is the introduction of a military-created standard for the operation of AWS.[190] This standard will set how such AWS may be used in accordance with the law of war.[191]

The establishment of such a standard operating procedure would also address accountability concerns by helping to establish a standard of care below which liability may be imposed on the human commanders of

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. CONGRESSIONAL RESEARCH SERVICE, DEFENSE PRIMER: U.S. POLICY ON LETHAL AUTONOMOUS WEAPON SYSTEMS (Dec. 19, 2019).

189. Press, *supra* note 71.

190. Benjamin Kastan, *Autonomous Weapons Systems: A Coming Legal "Singularity"?*, 2013 J. OF L., TECH. & POL'Y 45 (2013).

191. *Id.*

AWS.[192] This accountability would ensure, at least partially, that the confidence of commanders would be balanced and reasonable.[193] Establishing standards of design, maintenance, and operation would aid in providing expectations for personnel so that this balancing effort would not be an excessively difficult or time-intensive endeavor.[194]

Also, separate command responsibility doctrine for modern technology such as drones and AWS should be created. Keeping legal advisors at hand in establishing these regulations, and within the decision process when they are carried out, would also be valuable.[195] For example, Professor Keith Miller's *Moral Responsibility for Computing Artifacts: The Rules*, can be considered.

CONCLUSION

If AWS are to be treated with other weapon systems, then commanders and others within the chain of AWS design, maintenance, and operation should be culpable for the actions and potential IHL violations committed by AWS.[196] This Article outlined the legal theory of command responsibility. It examined the individual and state responsibility, and a test for determining command responsibility is conducted. Further, this Article discussed the intent and command responsibility, the international criminal law framework for AWS, and the search for criminal culpability. Finally, this research provided four solutions for command responsibility in relation to AWS.

192. *Id.*
193. Press, *supra* note 71, at 1365.
194. *Id.* at 1364.
195. *Id.* at 1365.
196. *Id.*