

What Existing Laws of Armed Conflict Apply to Autonomous Weapons Systems

Graham Overcash

On the battlefields of Libya, soldiers were targeted not by human adversaries but likely, by autonomous drones—heralding a new era of warfare. During the Second Libyan Civil War, “logistics convoys and retreating [Haftar Affiliated Forces] were subsequently hunted down and remotely engaged by unmanned combat aerial vehicles or the lethal autonomous weapons systems” (AWS).¹ These systems “were programmed to attack targets without requiring data connectivity between the operator and the munition ... a true ‘fire, forget and find’ capability.”² As these systems evolve, it is important to examine the current legal framework regulating armed conflict. While AWS are difficult to define, this blog will refer to the House of Lords Artificial Intelligence in Weapon Systems Committee definition: “weapon systems which can select, detect, and engage targets with little to no human intervention, or which possess some degree of autonomy in one or more respects.”³

Global military powers have developed, and anticipate the use of AWS in future conflicts, and thus oppose preemptive regulatory bans.⁴ An international legal framework must be created to ensure the responsible use of AWS in conflict. International legal frameworks, however, often require a long time to initiate. Even though AWS are a new and emerging technology, they are still bound by the traditional laws of armed conflict. United Nations (U.N.) governmental experts recently stated that “[i]nternational humanitarian law continues to apply fully to all weapons systems, including the potential development and use of lethal autonomous weapons systems.”⁵ This imposes several obligations on the users of AWS and provides a framework for accountability when used to breach international law. This blog will examine the prohibition of indiscriminate attacks using AWS, the obligation to perform a legal review of new weapon systems, and the positive obligations of distinction and proportionality.

The existing laws of armed conflict prohibit indiscriminate attacks that “employ a method or means of combat which cannot be directed at a specific military objective” and “are of a nature to strike military objectives and civilians or civilian objects without distinction.”⁶ The existing obligation against indiscriminate attacks is an important tool to prevent unintended engagements

¹ Panel of Experts on Libya Established Pursuant to Security Council Resolution 1973 (2011), Letter dated 8 March 2021 Addressed to the President of the Security Council, U.N. Doc. S/2021/229, at 17 (Mar. 8, 2021).

² *Id.*

³ AI in Weapon Systems Committee, *Proceed with Caution: Artificial Intelligence in Weapon Systems*, 2023-24, HL Paper 16, at 8 (UK).

⁴ Cong. Rsch. Serv., *The U.S. Defense Industrial Base: Background and Issues for Congress*, IF11294, at 1 (2023).

⁵ Guiding Principles Affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, U.N. Doc. CCW/MSP/2019/9, Annex III (Dec. 13, 2019).

⁶ Int’l Comm. of the Red Cross, Rule 12: Definition of Indiscriminate Attacks, Customary IHL Database, <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule12> [<https://perma.cc/QF56-4PP2>] (last visited Sept. 12, 2024).

targeting civilians. If the software directing an AWS is so poor that it cannot be directed at a specific military objective, then rates of harm to civilians could be high. Even if targeting is unintended, laws of armed conflict can be violated by employing a weapon so indiscriminate that it cannot distinguish between military and civilian objectives.

The prohibition against indiscriminate attacks highlights the importance of a comprehensive legal review. If during a legal review it is found that an AWS “is inherently indiscriminate,” then it “must not be used.”⁷ It is important that any weapon system can be directed toward a specific target, however, it is particularly important for AWS. Since AWS makes the targeting decision without human input, it must be capable of distinguishing between military and civilian targets. The prohibition against indiscriminate attacks is an important pillar of international law that promotes the responsible use of AWS, limits civilian casualties, and lowers the risk of unintended engagements.

States have a positive obligation to review new weapon systems for any potential illegal uses under international law. These legal reviews “are a useful tool to assess nationally whether potential weapons systems based on emerging technologies in the area of lethal autonomous weapons systems would be prohibited by any rule of international law applicable to that State in all or some circumstances.”⁸ If AWS use is considered, but during a legal review, the rate of unintentionally targeting civilians is unacceptable, there is an obligation to correct this issue before use in the field. States have considerable leeway in how legal reviews are conducted and an important obligation to comply with the laws of armed conflict before use on the battlefield.⁹ Comprehensive legal reviews are a key tool provided by international law to ensure that AWS are used responsibly in line with the existing law of armed conflict.

Finally, states have a positive obligation of distinction and proportionality. These principles ensure that a state takes precautions and steps to verify that the targets are military objectives and that the attack is proportionate to the posed threat. These principles provide an example of existing obligations that protect civilians from unintended engagements by AWS.

There are two elements of distinction when applied to AWS. First, “operators must have the intention of striking specific or potential targets that constitute military objectives.”¹⁰ Second, “the autonomous weapon system needs to perform with adequate reliability to enable, in the circumstances of its use, force to be directed against such targets.”¹¹ These two elements are

⁷ Guiding Principles, *supra* note 5, at Annex III.

⁸ Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Report of the 2019 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, U.N. Doc. CCW/GGE.1/2019/3, at 4 (Sept. 25, 2019).

⁹ *Id.*

¹⁰ Guiding Principles, *supra* note 5, at Annex III.

¹¹ *Id.*

designed to ensure that an AWS is only used against legitimate military targets and require that the system can distinguish between illegitimate civilian targets. To avoid violating this principle, states must rigorously develop and test an AWS that can consistently distinguish between an enemy combatant and a civilian during chaotic battlefield conditions.

Additionally, all attacks must be proportional to the objective targeted, this is especially relevant in areas where there may be a high concentration of civilians. The principle of proportionality requires that a “commander must not direct or authorize subordinates to use the weapon system when the commander has assessed that the expected loss of civilian life, injury to civilians, and damage to civilian objects incidental to the use of the weapon system will be excessive about the concrete and direct military advantage anticipated.”¹² In other words, if an AWS can identify legitimate military objectives among civilians but the destruction would lead to high rates of civilian casualties or damage to vital infrastructure, then the AWS cannot engage that target until the risk of collateral damage is lower. Even though the civilians are not the target of the attack, and a proper military target has been identified, the law would prevent such an attack to minimize unintended civilian casualties. This example highlights how the current laws of armed conflict can be applied to AWS.

AWS represents the future of warfare and highlights the need for a comprehensive legal framework designed to address the legal issues posed by these weapons. The development of AWS by the global military powers and the active use of AWS in war, highlight the immediate need for an AWS regulatory framework. In the meantime, however, the existing laws of armed conflict can be used to regulate AWS. Current laws of armed conflict, such as the prohibition against indiscriminate attacks, the obligation to conduct legal reviews of new weapons, and the principle of distinction and proportionality, can positively impact the responsible and legal use of AWS while a more permanent framework is developed.

¹² *Id.*