Is existing law adequate to govern autonomous weapon systems?

By

Dr Thompson Chengeta

1. INTRODUCTION

"*The way you fastidiously defended the sufficiency of international humanitarian law (IHL) in regulating the challenges of asymmetric warfare reminded me of the passion of a parent whose suitability is put to question in a dispute over custody of a child*". This was a comment by a judge on my submissions in the All-Africa IHL student Moot Court Competition organised by the ICRC. Back then, I believed in the adequacy of IHL to deal with the challenges posed at that time. Like many IHL scholars, I feared the risk of weakening of IHL rules through unnecessary adjustments.[1] Yet in this essay, if I am to be the same parent in a custody-case as likened by the judge, I am afraid that existing law is insufficient to fully cater for this new born —— autonomous weapon systems [AWS]! While there is no agreed definition, AWS are generally defined as robotic weapons that, once activated, can select and release harmful force without further human intervention.[2]

Through three examples, I seek to show — contrary to the views of some scholars[3] — that **AWS raise complex legal, ethical and operational issues that are outside the arm's reach of existing law**. The ICRC — an organisation considered to be the "guardian" of IHL — also points

[1] This was mainly in law of armed conflict as it relates to drone targeted killings and other counter-terrorism operations.
[2] UN Special Rapporteur Report, A/HRC/23/47, p. 7.
[3] ICRC, *Expert meeting on Autonomous weapon systems: Technical, military, legal and humanitarian aspects*, 26-28 March 2014, Geneva, Switzerland, pp. 8, 19,22.

to the insufficiency of existing law in its **recent publication of 6 June 2019**.[4] In this essay, existing law refers to all legal regimes applicable to AWS.

From the beginning, I emphasise that **questioning the adequacy of existing law to govern AWS is neither to deny its applicability nor is it to stigmatise all artificial intelligence [AI] technologies**. Rather, the argument is that **AI can only alleviate human suffering on the battlefield if it is adequately regulated and properly used**. Insisting that existing law is adequate when it is not only further endangers civilians and other protected persons.

The **question whether existing law can adequately govern AWS is critical because it is pivotal in the determination of an appropriate policy option on AWS**. Currently in the UN CCW, States are discussing possible policy options on AWS[5] and the major suggestions are a legally binding instrument[6] and a political declaration.[7] There are also a few States that have argued that existing law is sufficient and nothing additional is needed.[8]

2. *LACUNA* AND AWS

A comprehensive analysis of existing law that is applicable to AWS shows that the use of AWS presents a *lacuna* — a legal gap. A *lacuna* is "a situation where the absence of a law or legal norm prevents an inherently illegal situation from being addressed, or where the applicable

[4] ICRC, *Artificial intelligence and machine learning in armed conflict: A human-centred approach*, 6 June 2019.
[5] See CCW/GGE.1/2019/1/Rev.1, p.1.
[6] Suggested by 28 States in the GGE. Also, the United Nations Secretary General, Antonio Guterres, also stated that there should be new international law to ban 'machines with the power and discretion to take lives without human involvement', see *Secretary-General's message to Meeting of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems,* 29 March, 2019.
[7] CCW/GGE.1/2017/WP.4, France and Germany Political Declaration Proposal, 7 November 2017.
[8] See USA Submissions, CCW/GGE.1/2017/WP.6, 10 November 2017.

law is incomplete".[9] Further, Kammerhofer defines **a *lacuna* as the "absence of something that arguably ought to be there"**.[10]

Kammerhofer's definition mirrors the ICRC's observations that the **challenges raised by AWS go "beyond questions of the compatibility of AWS with our laws to encompass fundamental questions of acceptability to our values**".[11] Aside the general principles of international law and basic rules of IHL — the limitations of which are discussed below — there are no specific legal provisions that address some ethical concerns that are raised by AWS.

2.1 INADEQUACY OF EXISTING LEGAL REGIME ON NEW WEAPONS REVIEW

Currently, there are three cardinal rules of international weapons law [IWL] that are considered in the legal review of new weapons. These are prohibitions on weapons that are indiscriminate by nature[12], weapons that cause superfluous harm[13] and weapons that cause serious damage to the environment.[14] These rules have attained customary international law status and are part of Article 36 of Additional Protocol I on the review of new weapons.[15] They are the basis upon which a new weapon can be deemed illegal *per se* or a lawful weapon that can be used in compliance with IHL.

---

[9] See A/CN.10/2016/WG.I/WP.6, p.2.
[10] Kammerhofer, *Gaps, the nuclear weapons advisory opinion and the structure of international legal argument between theory and practice* (2009) 80.
[11] Ethics and autonomous weapon systems: An ethical basis for human control? International Committee of the Red Cross (ICRC), *Geneva, 3 April 2018,* p.7.
[12] Rule 71 of ICRC Customary Study; Art. 51(4) of AP I; Art. 8 (2)(b) of ICC Statute, Para 42 (b) of San Remo Manual.
[13] Rule 70 of ICRC Customary Study; Art. 35(2) of AP I; Art. 20 (2) of AP II; Preamble of CCW; Art. 3(3) Protocol II to CCW; Art. 8 (2) (b) of ICC Statute; Art. 23 (e) of 1899 Hague Regulations.
[14] Rule 45 of ICRC Customary Study; Art. 35 (3) and Art. 55 (1) of AP I.
[15] Art. 36 of AP I to the Geneva Conventions.

There are scholars and States that posit that once AWS are deemed compatible with the above three rules, then that must be the end of the debate. This is certainly not a true capture of all the concerns associated with AWS — in particular, **ethics and value-based concerns that go beyond what is found in existing law**.[16] As pointed by Kammerhofer, something that ought to be there is absent. With the advent of AWS, **the three IWL rules that were once an ultimate yardstick on the acceptability of a new weapon have become, unfortunately, an inadequate scale**.

The drafters of the above-mentioned **IWL rules did not anticipate weapons that carry computers that make decisions and legal judgments on the use of force** against humans.[17] Reasonably, they concerned themselves with review of new weapons that are nothing more than tools in the hands of fighters. They did not anticipate "*robo-combatans"* — a situation that arises in cases where weapon systems are fully autonomous.

The legal inquiry in terms of Article 36 is whether a weapon is lawful in terms of the three IWL rules and can be **used** by humans in compliance with applicable laws. The question i**s not whether the weapon or capability can, by itself, make lawful decisions on the use of force and carry out legal judgments associated with such decisions.** That duty has, from time immemorial, been the sacred preserve of humans. Thus, AWS enter uncharted territory where they threaten — or at the very minimum — question some of humanity's long held views and values.[18]

---

[16] ICRC [Note 11] p.5.
[17] Chengeta, *Are AWS the subject of Article 36 on the review of new weapons*, (2016).
[18] Simpson & Christopher, *Lacunae and silence in international space law - a hypothetical advisory opinion from the International Court of Justice* (2017); Morita, *The issue of lacunae in international law and non liquet revisited* (2017), pp.33-51.

Of course, there are States that have argued that under no circumstances can robots or computers make decisions to use force because they only execute pre-programmed human decisions.[19] According to this view, there is nothing far reaching about AWS to the extent of creating a *lacuna*. This view appears to be anchored on a misdirection of what human decision-making means when force is used.[20]

The decision to use force or to attack a human cannot be sufficiently pre-programmed.[21] Once a decision has been made, it has to be reviewed throughout the targeting cycle until the final release of force.[22] The IHL precautionary rule demands this.[23] As will be further argued below, the issue of decision-making and the notion of attack under IHL is problematic in cases where AWS are used.[24]

In terms of the existing legal regime, new weapons ought to be reviewed in terms of applicable laws, the applicable laws of which are inadequate. It is to this end that the ICRC has noted that while the current legal reviews of new weapons are important, "they are not a substitute for States working towards internationally agreed limits on autonomy in weapon systems".[25] **I suggest adding other rules to the existing three IWL rules — for example, the requirement of fixed, verifiable minimum level of human control over weapon systems**.

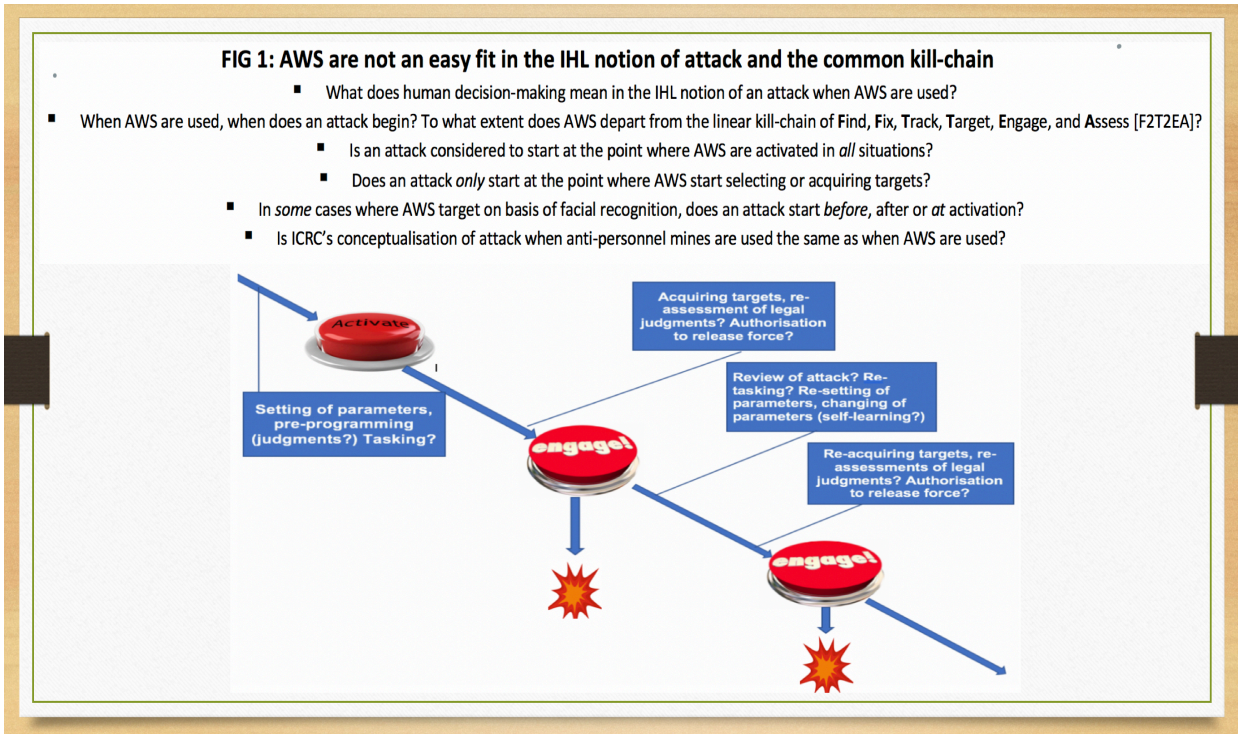
[19] This is one of the main arguments of the United States of America in the UN Group of Governmental Experts on Lethal Autonomous Weapon Systems.
[20] Chengeta, *Defining the notation of meaningful human control over AWS*, (2017).
[21] ICRC Statement to the UN CCW Group of Governmental Experts on Lethal Autonomous Weapon Systems, 25-29 March 2019.
[22] *Id*.
[23] Art. 57 of AP I.
[24] See Section 2.2.
[25] ICRC [note 21].

2.2 IHL NOTION OF ATTACK, TARGETING RULES AND AWS

The legal and ethical arguments that the decision to use force and the making of legal judgments associated with such force cannot be delegated to computers[26] are anchored on one's understanding as to when the use of AWS constitutes an attack. Likewise, **perceptions on the sufficiency or meaningfulness of human control exercised over a particular attack are dependent on where one thinks an attack begins and ends**.

More importantly, the application of certain IHL targeting rules also depends on where the attack starts and ends.[27] Yet, while IHL defines an attack as "acts of violence against the adversary", there is no indication as to when an attack begins.[28] In the past, there was no need for the law to pinpoint the beginning and end of an attack because weapons were unsophisticated and it was easy to locate when an attack starts. Yet, the questions in **Fig 1** below clearly shows this may no longer be the case where AWS are used.

[26]See ICRC [note 4].
[27] See Art. 57 of AP I.
[28] Art 49 (1) of AP I.



While existing unmanned systems such as armed drones have followed — with easy adaptation — the F2T2EA linear kill-chain within which it is easy to locate the start and end of an attack, the introduction of autonomy in weapon systems makes the kill-chain obsolete "to a point that questions the notion of the current looped-linear F2T2EA methodology".[29]

Autonomy in AWS introduces a complicated time/range paradigm where the kill chain is executed internally or via a network of other AWS presenting a multi-domain battle that is characterised by challenges of cross-domain synergies. Existing law did not anticipate this, and it has never been experienced before.

Some may argue that the question as to when an attack begins is not new in disarmament. When the question was asked in the case of anti-personnel mines, it was resolved that a mine

[29] Benitez, *It's about time: The pressing need to evolve the kill chain* (2017).

constitutes an attack when a person is endangered by it.[30] Yet, this "*endangerment threshold*" may not necessarily be helpful in the case of AWS which are more sophisticated and unpredictable.

Furthermore, an attack using mines is not a lawful attack that is contemplated in Article 49 (1) of AP I. The definition of an attack as "acts of violence against the *adversary*" in Article 49(1) *only* covers lawful attacks — those that are directed against legitimate targets. Under IHL, for one to be an *adversary* — against whom it is lawful to direct an attack — a person has to be a combatant or directly participating in hostilities. Depending on the level of autonomy, not all AWS attacks are unlawful as is the case with mines.[31] As such, AWS present a case of unchartered territories in as far as the question when does the use of AWS constitute an attack is concerned.

2.3 INADEQUACY OF EXISTING LEGAL RESPONSIBILITY REGIME

AWS create an individual responsibility gap for war crimes and other breaches of IHL.[32] Individual responsibility for crimes is premised on the legal assumption that it is humans who make decisions in an attack and the resultant acts are a manifestation of human intention. This assumption is not always true where AWS are used.[33]

---

[30] ICRC Report on the Meeting of the International Society of Military Law and the Law of War [Lausanne, 1982], para 1960 p.622; Maslen, *Anti-personnel mines under humanitarian law: A view from the vanishing point*, p. 190.
[31] Anti-personnel Mines Ban Treaty.
[32] Chengeta, *Accountability gap and AWS* (2016).
[33] HRW, *Mind the Gap* (2015).

Some have argued that an individual responsibility gap does not arise because whosoever activates AWS is responsible.[34] This view is a misdirection as it ignores settled criminal law principles on human intention and seeks to introduce a strange and an untenable notion of "strict individual liability" for war crimes.

3. *LACUNA* AND EXISTING GENERAL PRINCIPLES OF LAW

Some scholars argue that even if there may be a *lacuna*, it can be bridged by general principles of law. This argument was found unconvincing by the ICJ in the *Nuclear Weapons Case.* **While the ICJ noted the timelessness of IHL basic principles, the Court admitted that nuclear weapons presented a qualitative difference from other conventional weapons**. According to the Court, existing law neither "contain[ed] any specific prescription authorizing the threat or use of nuclear weapons".

Thus, **while courts sometimes fill in *lacunae* by applying general principles of law[35], they may only go as far and are not allowed to create law**. To this end, Judge Vereshchetin noted that where a "court finds a *lacuna* in the law or finds the law to be imperfect, it ought merely to state this without trying to fill the *lacuna* or improve the law by way of judicial legislation". Instead, **the Court emphasised the importance of express regulations in international law through new treaties where appropriate**.

Where there is a *lacuna* like in the case of AWS, inaction is not a viable option otherwise one risks the residual negative principle that provides that "what is not prohibited is legally permitted". After all, the attitude of governments bears witness to whether something is

[34] Dunlap, *Accountability and Autonomous Weapons: Much Ado About Nothing?* (2016).
[35] See the *Corfu Channel Case, the Atomic Bomb Trial and the Trail Smelter Case.*

considered unlawful and restrictions on States' conduct cannot be presumed but expressly stated in conventions.[36]

4. CONCLUSION

In conclusion, the shortcomings of the legal regime on the review of new weapons when reviewing AWS and the legal accountability gap that arises when AWS are used exemplify why existing law is insufficient to properly regulate them. This *lacuna* can neither be cured by ignoring it, engaging in creative interpretations of existing law nor putting in place political declarations devoid of legal force to bridge the legal gap. It is fundamental to have a legally binding instrument on AWS.

[36] See the *Fisheries* and *Lotus* Cases.