Legal Transplants: Applying Arms Control Frameworks to Autonomous Weapons

Berkant AKKUŞ

Abstract

The Geneva Conventions and Additional Protocols that regulate the law of armed conflict are insufficient to interpret autonomous weapon systems, which are among the modern weapon technologies that will be actively used by armies in the near future. This article focuses on autonomous weapon systems, which are not yet subject to regulation in terms of international law and which are still under debate with regard to prohibition in the global arena, and examines whether they can be an alternative for autonomous weapon systems by examining the regulations previously prepared on landmines, incendiary weapons, and cluster munitions through legal transplants. As a result of the conclusions reached in the article, recommendations will be shared on the content and legal status of the international humanitarian law manuals that should be prepared for autonomous weapon systems.

Keywords: Autonomous Weapon Systems, Artificial Intelligence, International Humanitarian Law

1. Introduction

Legal transplants refer to the legislative process whereby a law in one jurisdiction is adopted by another jurisdiction; frequently, such laws must be altered and customised so that they are aligned with the legal framework of the adopting entity. This term was invented by Watson and was originally employed to refer to the transference and adaptation of laws that address areas of similar concern between the legal systems of different nation-states (Watson, 1974). In the case of autonomous weapon systems (AWS), it refers to the search for regulations in extant legislation that control weapons that could be gainfully replicated within a treaty that regulates AWS or a voluntary compliance law of...
armed conflict manual. The United States Department of Defense (US DoD) is a prime example of this type of practice. It endorses “applying rules by analogy”, (The United States Department of Defense, 2016, s. 7) which adopts essentially the same process but on a comparatively informal basis. There are obvious advantages of transplanting laws or following rules by analogy: when regulations are already in place that have a proven record of success in the regulation of weaponry that has elements in common with AWS, they will almost certainly be easier to administrate and, as such, more successfully aid in the regulation of autonomous weaponry (Crootof, Autonomous Weapon Systems and the Limits of Analogy, 2018, s. 83).

Developments in military technology in recent years have led to the emergence of many new weapons, from cyber weapons to autonomous weapon systems, from drones to military human enhancement technology. International humanitarian law is insufficient for this rapid change. Therefore, this article will offer suggestions on how new military technologies should be regulated, with a special focus on autonomous weapon systems. However, this work has only examined the initial stages of a lengthy legal journey that lies ahead, which makes it problematic to select an absolute point of conclusion. The debate on the use of autonomous weapon systems is addressed from many perspectives such as ethics, international responsibility, international human rights law, international security, international humanitarian law, and international criminal law. This article, approaches autonomous weapon systems from the perspective of international humanitarian law and will present the results of the research on the axis of arms control. This article will basically consist of three parts. The first part will try to define autonomous weapon systems. The second part will examine arms control treaties and propose solutions in order to create legal transplants for new technologies. The last part aims to provide a guideline for autonomous weapon systems.

2. Defining Autonomous Weapon Systems

A good deal of the discussion related to the Convention on Certain Conventional Weapons (CCW) (Convention on Conventional Weapons, 2016, s. 3) process and other areas has become cantered on and to an extent fixated with different definitions of autonomous as applied to weaponry. Entities engaged in this debate should make strenuous efforts to create a definition of autonomy in this area that is supported by stringent analysis of legality and other issues. Debates regarding AWS regulation are essentially responsive to the technology available and how they will influence armed conflict in terms of deterrence, operations, and subsequent consequences. There is no possibility of states agreeing on substantive legislation without having an agreement regarding the problem they are addressing. To be specific, the concept of autonomy must be understood in line with the following points:

Autonomy for weapon systems refers essentially to the capability of operation without a human being directly controlling the weapon. Autonomy relates to the control. AWS does not refer to any particular form of weaponry that has a particular influence on targets, such as a blinding laser or mustard gas. Indeed, autonomy has no relation to the actual weapon in question; it simply relates to the control of the weapon (Caron, 2020, s. 175). The technology allowing for autonomy in a weapon system is generally an element of the weapon platform, although it will not necessarily even be attached to the weapon under control. AWS may employ numerous elements (sensors, radar, etc.) of an armed force’s battlefield and other resources.

The capability of a weapon system for autonomous operation varies between systems. Certain systems may have highly autonomous capabilities in some areas, e.g. navigation, but be less autonomous in other respects, e.g., target identification; autonomy levels could fluctuate at different operational stages or as circumstances vary (ICRC, 2016). Armed forces have been deploying weapons systems that have a limited capacity to operate autonomously for many years, and there is little debate
regarding their legal status. The critical functions approach brought to the fore by ICRC revealed the
crucial questions for those researching AWS generally relate to the capacity to select and engage a
target. Autonomy does not imply that a weapon is truly independent or not controlled by humans.
Although in certain instances human operators may have limited or zero capacity to modify the
operation of an AWS once activation has occurred. The human control element in AWS is essentially
part of the software design in the operating system (Chengeta, 2017, s. 852). The software takes the
place of human operators, controlling those elements of the weapon system where autonomy is
desired. But in future it may also be out of the algorithmic control.

In legal terms, it is not helpful to regard AWS in an anthropomorphic manner. Doing so implies that
AWS are not so much weapons as additional combatants. The regulations applying to AWS deployment
are identical to those regarding the deployment of other weaponry. The legal difficulties that AWS
pose are created by the extent of autonomous capacity how much autonomy the weapon is permitted,
how far human operators oversee and intervene with the weaponry, and the situations in which
autonomous operation is permitted. However, leaving the decision to kill entirely to machines results
in the dehumanisation of armed conflicts that undermines our values and the principle of humanity.

3. Regulating Autonomous Weapon Systems

Proposals for total bans on developing AWS based on international humanitarian law (IHL) cannot
be sustained either with reference to IHL as it currently applies to AWS or to the current state of
knowledge regarding the systems that are in development as far as they are publicly known. As yet
there is no suggestion that AWS, now or in the future, will become essentially indiscriminate, that they
impose suffering or injury unnecessarily, or that they will, by their very nature, cause legal violations.
Any weapons system has certain limitations in its capacity to comply with the law when selecting and
engaging targets (Blake & Imburgia, 2010, s. 159). Nevertheless, if a specific weapon system is not
capable of adhering to the law when attacking a target in a specific scenario, it is hard to conceive of
generalizing such limitations apart from prohibiting the specific weapon being used in a specific
scenario.

In order to ban AWS, there are difficulties of definition that must be dealt with. As different systems
are autonomous to different degrees, there is no one class of AWS that has a particular outcome for
targets as was the case for blinding laser weaponry that was successfully banned pre-emptively. There
are three difficulties with producing a definition of AWS that can successfully classify weaponry as
either autonomous or non-autonomous. Some definitions are excessively specific, detailing future
weaponry with human-style capacities that have yet to be developed (Ministry of Defence, 2011, s.
206). Other definitions are specifically technical, defining autonomy as a self-management capacity
that numerous extant weapon systems already possess and that do not focus on matters of legal
significance. Other definitions only address specific aspects of AWS, e.g. learning capacities, (Roff,
2014, s. 212) and these may become obsolete with technological developments, or may exclude
the weapon systems requiring regulation due to the other problems.

In fact, banning AWS may not be desirable in terms of humanitarianism. Even those who oppose
AWS acknowledge that higher precision levels and weaponry may be beneficial. The concept of benefit
refers not only to the military but in terms of humanitarian outcomes (Docherty, Losing Humanity The
Case against Killer Robots, 2012). Improved target identification, greater control over force levels, and
other superior capacities are part of the beneficial outcomes offered by future developments in AWS.

However, there are clear dangers in the pursuit of creating complex new technologies of enormous
use to the military. In that, the desire to reap the benefits of the new technology may, without proper
regulation, make the creators and/or users of such weaponry behave in undesirable ways. As
demonstrated by the CCW debate, and that amongst the wider public, many people are uncomfortable with the concept of machines being given the authority to decide on the use of lethal force, even if it is effectively simply following human orders (Ülgen, 2020, s. 8). A substantial body of opinion regards developing AWS as undesirable on ethical, moral, legal or other grounds. The mere fact that a risk is perceived to exist might be the foundation upon which a legal regulation could be built: “All existing prohibitions on conventional armaments stem from the conviction that the use of the kinds of conventional weapons described bears the unacceptable risk of violating the most fundamental principles of humanitarian law.” (Dekker, 2001, s. 79)

It should be decided to implement specific regulations for developing and deploying AWS, at the same time caution should be used in their application. Regulation should be rooted in clear comprehension of what AWS is and should offer careful measures related to clear and specific risks and should ensure that innovation that could be genuinely beneficial is not stifled. Anderson and Waxman have noted that it can be beneficial to regulate systems as they are invented, and that this is possible. However, regulation must be created as the technology is created, and in future autonomous technology will become more and more commonplace, e.g., with self-driving vehicles, and robots for caring for the elderly or undertaking nursing functions. In much of this technology, machines will be given the capacity to behave in ways that could potentially be lethal. Generally, as an agreement is reached that machines may be superior to humans in undertaking particular tasks (Anderson & Waxman, Law and Ethics for Autonomous Weapon Systems: Why a Ban Won’t Work and How the Laws of War Can, 2013, s. 3).

As the regulatory process has already commenced in the CCW context, useful guidance may be derived from the examination of the contents of CCW Protocol II. This Protocol has a number of elements that could offer an applicable foundation for AWS regulation.

Firstly, CCW Protocol II refers to the general principles of IHL and stresses that they are equally applicable to the deployment of mines and, if relevant, refers to the particular rules that apply: Article 3 (3) (superfluous injury/unnecessary suffering); articles 3(8)(a), 3(8)(b) and 3(9) (distinction); article 3(8)(c) (proportionality); article 3(10) (precautions); and article 3(11) (warnings).

Secondly, the Protocol recognizes the particular risks caused by the deployment of mines and orders particular ways of addressing said risks. To prevent the inadvertent entry of civilians into areas where mines are present, article 5(2)(a) states that mines have to be “placed within a perimeter-marked area which is monitored by military personnel and protected by fencing or other means, to ensure the effective exclusion of civilians from the area.”

Thirdly, the Protocol establishes positive regulations to create the maximum level of protection: in Article 11 every signatory promises to offer technical support and assistance to assist all other signatories in the implementation of the Protocol. This assistance includes providing equipment, expertise, and sharing information.

Fourthly, the Protocol, in its technical annex, offers a wealth of technical information that gives support to primary rule implementation.

It is too soon to specifically define what rules should be included in a similar Protocol for AWS. As yet, states have not come to an agreement on whether AWS-specific regulation is required. It should be agreed that regulation is required, the first order of business will be to define the aims of the regulation (guidance, restriction, or prohibition of deployment or development) and to create a definition of which weapon systems/technology come under regulation prior to formulating a set of substantive rules.
This is a new legal area and, as AWS are still an embryonic technology, it is necessarily in constant flux due to major advances in technology. We know enough to recognize that giving autonomy to lethal weaponry raises problematic questions, but as yet we have insufficient knowledge to provide conclusive answers to said questions. Further research is required into every area of international law and warfare that AWS development will influence. Hopefully, this article offers some guidance as to how questions of IHL and AWS may be answered.

It may be best to end by simply exhorting all actors to continue their close engagement with the developers/potential users of AWS in order to comprehend the problems they pose to the achievement and maintenance of international law, and to create solutions for them. There are three particular regulatory frameworks that may prove profitable in offering broad guidelines for efficacious and practical regulation, those applying to landmines, incendiary weapons, and cluster munitions.

3.1. Landmines

Landmines are regulated by the Ottawa Convention (Mine Ban Treaty)\(^2\) and the Amended Mines Protocol\(^3\). The Ottawa Convention introduced a ban on antipersonnel mines, although a number of the most significant military powers, including China, Russia and the USA, are not signatories. Big military powers in the world have been claiming it is militarily necessary for them to retain such capacity (Capece, 1999, s. 183). The Amended Mines Protocol regulates deployment of landmines and is effectively adhered to by those states that did not sign the Mine Ban Treaty (Bryden, 2013, s. 87). It should be noted that this assessment is not shared by everybody and some non-governmental organizations (NGOs) would dispute this. AWS and landmines are similar in that, post-deployment, they will choose and attack objectives without needing further input from personnel. As an example, anti-tank mines incorporate pressure sensors that allow them to make a basic distinction between a vehicle and a human being on the basis of their weight; for this reason, Article 2 (1) of the Mine Ban Treaty specifically leaves anti-tank mines out of its regulations, though it still includes anti-personnel mines. In fact, the extent to which a weapons system can distinguish between targets is an essential element of its compliance or otherwise with IHL (Lewis, 2015, s. 1309). In addition, the Amended Mines Protocol has certain caveats that acknowledge that fields of operation may impose different requirements and adapts itself to these in terms of regulation. Examples are:

The Protocol does not apply to anti-ship mines deployed on the high seas, given that large concentrations of civilians are not likely to be present (provided the weapons are not placed in commercial shipping lanes), and so naval commanders generally do not have to consider proportionality or distinction problems. In line with the analogy between mines and autonomous weapon systems, autonomous weapon systems can be used in military bases or border control operations in line with the marking and determination of the areas where these weapons will be used. In autonomous weapon systems with mobility and flight capability, sensors can replace humans for the task of monitoring civilians and civilian areas. Of course, the nature of the monitoring should be determined carefully and privacy should not be violated.

The Protocol does not allow landmines to be placed in or around objectives that would usually be employed by civilians; e.g., places of worship, schools or homes. In line with the applicability of this provision to autonomous weapon systems, it can be ensured that these weapons can only be deployed in areas where civilians are not densely populated, such as deep sea, deserts, and space. For instance,

---


urban and protected areas can use geofencing in order to create a no-fly zone that prevents autonomous weapon systems from targeting civilian objects and civilians. Alternatively, cultural assets are indicated by the blue shield and the distinctive emblems of the Red Cross and the Red Crescent are recognised worldwide. In this respect sensors of autonomous weapon systems can be designed to detect these distinctive symbols.

The Protocol does not permit target area emplacement, i.e., grouping a number of unique military targets into a single target; this means that a greater level of specificity is demanded in areas that may contain a mixture of civilian and military objectives. Analysing the autonomous weapon systems used as swarms in accordance with this provision reveals that autonomous weapon systems can be used in swarms to destroy many targets in the city (Boogaard, 2015, s. 276). Micro-drones that operate coherently can be part of the swarm. Even if each attack is assessed separately and the damage to civilians and civilian structures is considered proportional, the damage caused by the swarm should be assessed collectively when calculating collateral damage because of combined attacks will cause collateral damage such as fire. Finally, autonomous weapon systems should not decide on proportionality without a human military commander. Because at this stage, the decision requires the evaluation of many strategic and political factors.

The Protocol insists that anti-personnel landmines must be capable of detection so that when clearance is necessary, they can be more easily discovered. Based on this provision, autonomous weapon systems can be designed to use electronic footprint technology during the targeting process. With the electronic footprint technology, which has a structure similar to the black box technology in aircraft, it will be possible to determine who makes the decisions (Sassóli, 2014, s. 338). Thus, clarification can be offered to prevent the problems created by autonomous weapon systems in terms of accountability.

The Protocol demands that anti-personnel mines should have mechanisms for self-destruction or deactivation effectively an automatic limiter. Alternatively, if they do not, that they must only be deployed in a controlled area that is clearly marked and patrolled by military operatives. If this provision is applied to autonomous weapon systems, autonomous systems that can distinguish between civilians and combatants should be considered safe. In this direction, systems that fail to distinguish between civilians and combatants will be considered unsafe and measures will be taken to prevent their use. In addition, it would be appropriate to remove the autonomous weapon system from the area after the attack has occurred. The use of sensors of autonomous weapon systems for intelligence gathering is one option, but the constant presence of aerial military systems in the region could cause psychological disturbance. In this case, psychological harm may be considered a violation of the prohibition of causing unnecessary suffering under international humanitarian law (Cavallaro, Sonnenberg, & Knuckey, 2012).

The Protocol restricts the deployment of mines that can be delivered remotely i.e., via artillery/aircraft, and imposes a requirement for care with these weapons; for example, wherever possible, advanced warnings should be issued to civilians in a targeted area. The obligation of advance warning of attack may be interpreted in line with the kill switch (Farge, 2021). Kill switch is an alternative method for integrating meaningful human control into autonomous weapon systems. Autonomous weapons communicate with the nearest mobile network stations via a sim card embedded in their systems, so that autonomous weapons can be disabled remotely if they are hacked or stolen by non-state armed actors, or if they start disproportionately attacking civilians.

These regulations from the Amended Mines Protocol, have the potential to be transplanted into other regulatory regimes. There are three areas for which the potential is obvious. Firstly, it has been argued by Klein that AWS could be restricted to military emplacements and quite small combat zones.
through the use of kill boxes, i.e.: “a geographic area defined by specific three-dimensional coordinates is designated, within which military objectives can be engaged once properly identified and after weapon release authority is given.” (Klein, 2004, s. 7)

The concept of kill boxes was invented by the US Air Force towards the end of the 1980s, and they have been used with success in many operations beginning with Desert Storm; they are extremely effective in effecting the coordination of joint weapons fire, permitting all three divisions of a military force to share attack duties, and engaging the enemy while protecting allies (Mullin, 2008, s. 38). Thus, AWS could be restricted to operating within kill boxes; the Amended Mines Protocol offers suggestions as to how this could be made legally obligatory where applicable.

The second regulation that could be transplanted from the Amended Mines Protocol is one that relates to the way in which anti-tank and anti-personnel mines are treated differently. In the same way, AWS could be distinguished by whether they are intended to attack material or personnel, with the regulations demanding greater control in the case of personnel targeting. Perhaps even being extended, in some situations, to man-in-the-loop requirements should be maintained (Canning, You’ve Just Been Disarmed. Have a Nice Day!, 2009, s. 12). The flipside of this would be that AWS operating fully autonomously in a combat zone would be programmed to the attack “either the bow or the arrow, but not the human archer.” (Canning, Weaponized Unmanned Systems: A Transformational Warfighting Opportunity, Government Roles in Making it Happen, 2008, s. 23) That is, AWS would only be targeting the military material and not the personnel. Although naturally it is impossible to prevent military personnel, or even civilians, suffering injuries or fatalities as a result of collateral damage.

The final potentially transplantable regulation relates to Articles 57 and 58, AP I. The Amended Mines Protocol is heavily influenced by Article 57 in that it demands “effective advance warning shall be given” for “any emplacement of mines”, or “any delivery or dropping of remotely-delivered mines”, that may impact upon civilians, unless it is impossible to deliver such warnings. Although this stipulation has feasibility caveats, it can be argued that its phrasing refers to the use of mines in many circumstances, and not just in specific kill zones, which are dealt with by another section of the Protocol. That being the case, a force deploying AWS may be obliged to provide a general warning along these lines and, thereby, oblige the enemy to adhere to the provisions of Article 58 (Dinstein, 2016, s. 122). Obligations under this article might include taking additional precautions that will help AWS to discriminate between targets; e.g., through deploying internationally recognized signage and emblems as appropriate. Furthermore, the defending force may have to offer attackers the GPS coordinates of protected locations e.g., schools, hospitals, enabling the attackers to add them to a no-strike database that controls the areas in which AWS may not be deployed.

It is arguable that the distinction between different types of landmines, their deployment, and the safety measures that must be employed during deployment, are a result of aspects of these weapons that are similar to aspects of AWS, i.e., that they can attack an objective without being under direct narrow loop control from a human being. This is why the Amended Mines Protocol emphasises the importance of the decisions taken by commanders, and the deployment of appropriate and graduated safeguards for the protection of civilian populations. In effect, the Amended Mines Protocol deals with issues that are very close to those raised by AWS, and so may offer many potentially transplantable regulations (Lewis, 2015, s. 1309).
3.2. Incendiary Weapons

With regard to incendiary weapons, Protocol III to the CCW may be useful. This is a small piece of legislation that creates regulations that may be transplantable for a AWS regulating treaty or LOAC manual. One notable provision is that it imposes a total prohibition on airborne incendiary weapons being deployed against military objectives when said objectives are within areas inhabited by civilians, as incendiary weapons have the potential to create firestorms that will harm all humans within the target zone, causing disproportionate civilian casualties. There is also a restriction on land-based deployment of incendiary weapons: When attacking military objectives surrounded by civilians, the military objectives must be clearly distinguishable from civilian concentrations, and every possible safeguard must be deployed to ensure that the incendiary weaponry only damages the military objective, with avoidance or minimisation of damage to collateral entities.

The Incendiary Weapons Protocol effectively acknowledges that due to the swift and unpredictable nature of fires, which are often at the mercy of the wind and other environmental elements, incendiary weapons tend to be indiscriminate post-deployment. The Protocol specifically bans all types of deployment that do not make the distinction between military objectives and civilians or in which unacceptably high civilian casualties occur as collateral damage. The Incendiary Weapons Protocol imposes sensible limitations on employment and deployment of incendiary weapons. These limitations may be applicable to AWS with rudimentary visual recognition capacity, and so these regulations may be transplantable to a AWS regulation treaty or LOAC manual.

3.3. Cluster Munitions

Another treaty worthy of consideration is the Convention on Cluster Munitions (CCM). This has a number of provisions that could be profitably transplanted (Docherty, Maresca, Reiterer, & Moyes, 2010, s. 245), and is, therefore, worthy of further study. In common with the Mine Ban Treaty, Article 1 of the CCM creates a rigorous and clear regulation, which in its breadth would appear to effectively ban cluster munitions. It is worth noting that Article 2(2)(c) goes on to permit technical developments, which the lead to the sub-paragraph suggests should “avoid indiscriminate area effects and the risks posed by unexploded sub-munitions.” It achieves this by omitting weapons possessing five unique technical elements from any definition of cluster munitions, these elements being those intended to improve accuracy and reliability (Breitegger, 2012, s. 193). Cumulatively, these elements should obviate, or at least adequately mitigate, the chance of sub-munitions causing unacceptable humanitarian suffering, dependent upon the specific circumstances. This subparagraph can be taken as relating to the second preambular clause, where state parties agree that they are: “Determined to put to an end for all time to the suffering and casualties caused by cluster munitions at the time of their use, when they fail to function as intended or when they are abandoned.”

Thus, the joint humanitarian difficulties regarding cluster munitions are defined as “indiscriminate area effects” when deployed, and the “risks posed by unexploded sub-munitions” when they malfunction or are left in situ post-conflict (Docherty, Maresca, Reiterer, & Moyes, 2010, s. 236).

By defining a pair of humanitarian issues that the technical elements later mentioned are supposed to avoid, the lead-in to subparagraph (c) serves two important purposes. It offers “both a justification for the exclusions of weapons that meet the […] technical criteria and also a potential mechanism for determining if these technical criteria function as intended.” (Docherty, Maresca, Reiterer, & Moyes,

---

5 Article 2(2), Incendiary Weapons Protocol.
In other words, the lead-in establishes a link between things that are banned and the humanitarian reasons for them being banned, which is a notable and novel legal move. Although cluster munitions are not specifically intended to cause humanitarian difficulties, paragraph (2)(c) states that, in order to avoid being banned, sub-munitions must possess specific design features that are intended to militate against such results. As such, the subparagraph in its entirety is concerned with both design and consequences, through the addition of the technical criteria and lead-in.

At the Oslo Process negotiations, the attendees felt it necessary to apply this to sensor-fused weaponry, which was seen as having the potential to offer the desired capabilities to military forces, and did not, at that time, have a record of causing humanitarian difficulties (Breitegger, 2012, s. 195). It could be argued that AWS require the same sort of provision, as they have yet to be deployed but are seen as possible increases of force, and they are still central to the Third Offset Strategy (Kerr & Szilagyi, 2016, s. 365). So we could agree that AWS are legal under international humanitarian law if they fulfil certain mandated technical requirements. However, this legality could be challenged should they be found to cause obvious humanitarian difficulties when deployed; this would appear to be a pragmatic and sensible accommodation, even though it is the reverse of the previous principles of the IHL (Wagner, 2014, s. 1369). Most importantly, it would seem to find a middle ground between the demands of military operations and requirements for humanitarian law (Egeland, 2016, s. 90).

Thus, employing this novel instrument Article 2(2)(c) may mitigate the fear that AWS could, in future, be unleashed into combat zones without adequate controls. At present, experts are not in agreement as to the sophistication and reliability of the algorithmic target construction systems (ATR) that may be introduced in future. Some are of the opinion that such weaponry will never have the capability to make a distinction between combatants and civilians, (Sharkey, 2012, s. 787) while others consider this may be a possibility; (Schmitt & Thurnher, 2013, s. 231) a third group are more pragmatic, seeing the limitations that presently exist as simply a technical challenge that may be overcome by computer scientists and robotic engineers (McFarland, 2016, s. 1314). If we adopt this third way—and we must always remember that it is extremely difficult to predict technological developments—then it would certainly not be the place of lawyers to make decisions regarding what may or may not be technically possible in future, and certainly not to assume that technical limitations cannot be overcome (Grace, Salvatier, Dafoe, Zhang, & Evans, 2018, s. 748). The task of the lawyer is to set out the legal and humanitarian safeguards that must be built into ATR systems and similar offensive weaponry so that they are compliant with IHL; it is then up to the scientists to create systems that fulfil the established criteria. Such a methodology would be particularly applicable to autonomous weapon systems because technology is moving so fast that the CCW diplomatic efforts have completely failed to keep pace with it and, should any treaty regulating AWS come into being, it is perfectly possible that its technical stipulations will already have been superseded and made obsolete. So, if a regulation based on Article 2(2)(c) CCM was created as part of a AWS regulation treaty or LOAC manual, it could do much to clarify this complex question.

In the first place, such regulation could set out the humanitarian problems with AWS that are not effectively designed or that in some other way are unsuitable in terms of meeting regulations. This could include weapons that offer risk of indiscriminate attack, distinction failure and insufficient civilian risk mitigation, as well as other problems. Subsequently, autonomous weapon systems containing design features that obviated or minimised these risks would be presumed to have legal status.

In the second place, such a regulation may incorporate provisions for specific technical requirements. These will chiefly comprise the minimum technical demands in terms of sensors, processing and computer power needed to mitigate specific humanitarian problems. The regulation could go further in setting out particular demands for programs dependent on context; it could
mandate the situations in which the weaponry should automatically shut down; and it could demand that when a weapons system is unsure of the nature of a target that it should alert a human controller who would remotely assume responsibility; this could be achieved by setting the weapon system to do this before the confidence level threshold is reached (Henderson & Backstrom, 2012, s. 492).

Finally, as AWS have never been subject to battlefield deployment, the mandated technical specifications may be regularly matched up with the perceived humanitarian dangers, to make certain that the weaponry will perform as desired. If it does not, the technical specifications could be periodically amended, possibly by presenting evidence-based data to a Review Conference or a Meeting of State Parties should a treaty have been agreed. It can be reasonably argued that between such reviews, state parties would still have a duty to make all reasonable efforts to assess the humanitarian risk from particular AWS by employing on-board sensors. State parties have to cease deployment if it becomes obvious that the weaponry poses an unacceptable level of humanitarian danger.

All these requirements are incorporated into the lead-in and technical specifications in Article 2(2)(c). If these requirements were transplanted into a AWS-regulated framework and suitably adapted, they could be perceived to offer states and weapons manufacturers the appropriate guidance and limits to make sure that autonomous weaponry remained legal and was continually being refined to minimise humanitarian risk. A specific mandate for regular reviews and amendments as necessary would, if fully adhered to, allow signatories to fully exploit cutting-edge technology, continually strengthening humanitarian safeguards without sacrificing military requirements.

There is a risk that these guidelines in isolation could make the situation seem less complex than it really is. As such, four things should be kept in mind. Firstly, it is problematic to verify specific technologies, particularly in terms of analysing, and incorporating safeguards into, software (Gubrud & Altmann, 2013, s. 2). Such amorphous technologies cannot simply be evaluated from an external inspection of weaponry (Crootof, The Killer Robots Are Here: Legal and Policy Implications, 2015, s. 1837). However, as inspectors would be focused on the verification of compliance with minimum technical requirements, rather than verifying the presence or otherwise of autonomous capability, inspectors could satisfy their remit through observations of training exercises or other practical demonstrations. It would still be difficult to make these inspections fully satisfactory, as it is simple to change a weapon’s capabilities any time by “throwing a software switch” (Gubrud & Altmann, 2013, s. 2); i.e., inspectors would only be able to observe the technical capability of a weapon that the operators wished to let them see.

Secondly, the CCM and the regulations that can be transplanted only contain prohibitions on particular sorts of technology on the basis of their design and/or the humanitarian risks they pose; there is no provision for the legal deployment of any weaponry. This means that any AWS that satisfied the regulations would still come under the aegis of the IHL attack rules; simply because a weapon appears to be legal in general terms, it cannot be assumed that it can be deployed in any circumstances, e.g., areas containing high levels of civilian population (Docherty, Maresca, Reiterer, & Moyes, 2010, s. 167). This is relevant in terms of previous suggestion that states should be obligated to continually monitor the results of AWS deployment and to take steps to mitigate any humanitarian risk that does arise.

Thirdly, if we expect states to monitor their weaponry and take appropriate remedial action to mitigate humanitarian risk, with cluster munitions and landmines there have been considerable problems in this regard. Predictably, given that the regulations have international reach, each state – each with differing priorities and each regarding IHL and arms control in a different light – do not exhibit uniform adherence to the Protocols. The levels at which different states monitor and modify
their weaponry in response to humanitarian risk have not been consistent, (Bryden, 2013, s. 93) and a great deal of the positive pressure on non-compliant states has come from NGOs, like the International Campaign to Ban Landmines (ICBL) and the Cluster Munition Coalition rather than the Protocols themselves. Although it is not impossible to imagine states being able to monitor humanitarian risks entailed by AWS, and refusing to deploy them in areas where the humanitarian risk will be unacceptably high, it may be argued that such a regime could only effective if NGOs, like the International Committee for Robot Arms Control, will be heavily involved in monitoring and reporting functions.

Finally, we must accept the possibility that all efforts to control autonomous weaponry may eventually come to nothing (Altmann, 2013, s. 137). It is highly likely that once the rubicon of the deployment of autonomous weaponry on the battlefield has been crossed, a new arms race based around AWS will commence (Sparrow, 2009, s. 25). However, we must assume that, in general, the design and usage of AWS, and their adaptation, will comply with IHL. If this does not happen as expected then, considering the usefulness of this weaponry in military terms and its capability to massively increase available force, it would be overoptimistic to assume that AWS would cease to be an element of national military capabilities. This total non-compliance may happen, but as, realistically, there is no great hope of a blanket ban on autonomous weaponry proving workable, regulation similar to Article 2(2)(c), CCM, seems the best approach.


Article 38 of the Statute of the International Court of Justice (ICJ) is the starting point for analyzing the sources of international law. Legal academics and international lawyers are actively involved in the interpretation of international law. For this reason, the correct approach would be to examine Article 38 (1) (d) of the Statute of the ICJ with regard to the extent to which legal scholarship contributes to the formation of international law. Judicial decisions and publications of scholars are a tool for determining the rules of law. Therefore, manuals can be considered as subsidiary means for the determination of rules of law under Article 38 (1) (d) of the Statute of the ICJ. In international law, treaties and IHL manuals differ in their normative status. Treaties, whether individual instruments or new Protocols in the Convention on Certain Conventional Weapons (CCW), are acknowledged as binding sources of international law (Shaw, 2017, s. 81). Contrastingly, IHL Manuals represent a “subsidiary means for the determination of rules of law”, (Crawford, 2015, s. 23) so while they are very useful in terms of guidance and interpretation, they are not binding. Due to this simple fact, treaties can be regarded as being more effective in terms of complying with IHL.

It is not possible to envisage artificial intelligence and full autonomy in weapons during the negotiation stages of the Geneva Conventions therefore the basic rules of international humanitarian law are designed to be applied by humans, not machines. While the relevant provisions of international humanitarian law apply to international armed conflicts however the changing nature of armed conflicts has made it crucial to constitute manuals that can also be applied to non-international armed conflicts or law enforcement operations. However, treaties are frequently not as comprehensive as IHL Manuals, because the parties involved generally want to avoid being bound to specific inflexible legal commitments, particularly in emerging areas. It may be argued that this will make an AWS regulation treaty less effective, as potentially the only agreement that could be reached would be a broad categorization of systems and deployment rules with vague provisions or ones with

---

many caveats, such as the Protocol V to the CCW. The only part of Protocol V that contains detail and precision is the non-binding Technical Annex, containing “voluntary best practice.” Additionally, the entire instrument including the Annex is just 14 pages long; IHL Manuals are generally much more detailed, with hundreds of pages of guidelines and specifics; the AMW Manual (Program on Humanitarian Policy & Conflict Research at Harvard University, 2009) comprises 56 pages, in comparison to the Tallinn Manual 2.0 (Schmitt, 2017) that comprises an astonishing 598 pages. Without interested parties applying political pressure to omit specific legal restraints, the manuals may provide better insights and guidance regarding the application of IHL in specific areas, entrusting commanders with the application of regulations as they apply to particular deployments.

Another option might be that one group of states and non-governmental organizations (NGOs) could produce a detailed collection of proposals for a treaty, hoping that other states would ultimately fall in with their proposals. In this way both detail and legally binding obligations could be produced. However, at present the members of the CCW are at loggerheads regarding future progress with AWS, and certain nations do not respond to pressure from NGOs, (Garcia, 2017) and so the prospects of this may be remote. Indeed, going down this route may result in AWS becoming a “Balkanized sector of weapons law”, (Watts, 2016, s. 187) with important users of AWS opting out. This, in fact, was the end of the Ottawa Process: although a comprehensive Mine Ban Treaty was produced, a number of states including South Korea, China, Russia and the US refused either to participate and/or to become signatories, even though they are generally voluntarily compliant with the treaty’s requirements (Docherty, Breaking New Ground: The Convention on Cluster Munitions and the Evolution of International Humanitarian Law, 2009, s. 945). Naturally, a treaty for the regulation of AWS would not amount to a complete ban on autonomous weaponry; it would provide clarification for the terms of deployment and usage. However, we must look at the context in which treaties are written: when the Ottawa Process commenced, antipersonnel mines were already less militarily useful than they had been in the past, and so many states were more amenable to their being banned. Contrastingly, many states are recognizing the potential effectiveness of AWS in future, and so it is probable that even larger numbers will decline to become signatories to a treaty that circumscribes their future activities, and thus weapons law could become “Balkanized.”

This leads us to return to the conclusion that an expertly compiled IHL Manual for AWS has the greatest potential for effective success by combining specific regulation, flexibility, and detail. These elements would make a Manual have a greater likelihood of being adopted and complied with across a broad range of states deploying AWS.

Thus, we can list the potential benefits of an IHL Manual for AWS as being: Providing authoritative expert interpretation and guidance, particularly with reference to the application of international law to the latest generation of weapon systems, with inputs from all appropriate disciplines. Filling the lacunae in treaty law in relatively quick order, free from the procedural and political complexities of creating a treaty. Having non-binding status, so that it can go into greater detail, providing commanders and legal advisors with a useful expert overview of regulations, principles, and guidance. Being non-binding, it has a greater likelihood of adoption by global military powers, who will be able to enjoy greater flexibility in the application of the regulations, principles and guidelines. All of the above will offer more standardized approaches to the deployment and employment of AWS in terms of compliance with the law, for both NATO and non-NATO forces.

In due course the standardization offered by such a manual may create fresh customary international law regarding autonomous weaponry, particularly if the regulations, principles and guidance of the manual become incorporated into the military documentation of states. The formation of custom in international humanitarian law is a process that takes a certain amount of time, and therefore the formation of international humanitarian law is largely dependent on state practice.
However, states are reluctant to state on highly debated areas of international humanitarian law such as cyber warfare, autonomous weapon systems, space warfare, and military human enhancement. The reason for this reluctance is, of course, the desire to limit themselves less in armed conflicts. Therefore, states generally prefer a wait-and-see approach instead of explaining *opinio juris* on developing areas of IHL (Schmitt & Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, 2015, s. 211).

### 4.1. The Potential Shape of an IHL Manual on AWS

If we are to create a manual that fulfils the aims expressed above, we should now examine the headings it might contain. All such headings would be created with input from many disciplines and experts in international law, human/machine interactions, weaponry design, cognitive science, software engineering, and robotics.

Such a manual would be divided into eight wide-ranging chapters. The first chapter would outline central definitions regarding AWS, e.g., autonomy and the difference between online learning and offline learning. It would also detail essential IHL definitions, including military advantage, collateral damage, and military objective. A crucial part of such a section would also provide a detailed description of the standards for meaningful human control (MHC) and what it might comprise, to provide references for other sections.

The second chapter would offer a general framework confirming that AWS fall under current IHL and other applicable international law and that they are *not de facto* illegal; however it would also explain that participants in armed conflict do not have limitless freedom to choose their own methods of warfare, and so AWS must comply with the standard legal requirements of legal review (Anderson, Reisner, & Waxman, *Adapting the Law of Armed Conflict to Autonomous Weapon Systems*, 2014, s. 386). This chapter would also offer an explicit affirmation of the fact that the manual restates extant treaty and customary law, operating without prejudicing extant national treaty obligations.

The third chapter would deal with weapons law, restating the regulations regarding the prohibition of weaponry that by nature or design will produce unlawful outcomes. This chapter could also incorporate regulations and policy guidelines for developing AWS, e.g. issues such as the incorporation of kill switches or self-neutralization mechanisms in such weaponry. It could also detail the minimum sensory requirements/processing capability required for AWS to allow them to make decisions with a reasonable amount of foresight and distinction. Furthermore, this chapter could reaffirm that customary law demands legal review; an outline of the ways in which this will be accomplished could be detailed, e.g. requirements for multidisciplinary review panels.

The fourth chapter would be a *jus ad bellum* chapter discussing scenarios where the choice to deploy force could be influenced by the availability or otherwise of AWS. This would extend the remit of the manual further than IHL matters. However, this is justifiable and appropriate if a weapon system poses a genuine risk to the *ad bellum* framework or threatens to complicate or obfuscate the way it is applied (Schmitt, 2017). Within the context of AWS, the most recognized threat to the *ad bellum* framework is the potential of a “flash war.” (Scharre, 2016) This can happen when opposed armies of AWS on peacetime deployment may come in close proximity to each other and recognize that they are both on high alert when searching for signals of impending aggression. In this situation, AWS from one side could be responsible for misinterpretation of non-aggressive manoeuvring by AWS from the other, which could then trigger a rapid pre-emptive military strike, with a subsequent counter-strike and rapid escalation of hostilities (Grimal & Sundaram, *Combat Drones: Hives, Swarms, and Autonomous Action?*, 2018, s. 117). Should this occur, there could be extreme uncertainty regarding whether the
first offensive action represented unlawful aggression or territorial violations or whether it was a legitimate pre-emptive self-defensive act (Grimal & Sundaram, Cyber Warfare and Autonomous Self-defence, 2017, s. 339). The manual could anticipate such issues by offering recommendations for safeguards against such machine-led incidents, e.g., it could detail scenarios where the attack parameters should be tightened, recommend the implementation of shoot second policies, and possibly recommend that some non-classified elements of control algorithms should be shared between states so that their AWS systems are more compatible in peacetime.

The fifth chapter would address law of targeting, i.e., how AWS can be deployed in a way that is compliant with the regulations and principles of distinction, proportionality, and due precautions. In this mooted fifth chapter, the IHL Manual could profitably incorporate these features: Clarification that distinction/proportionality decisions are taken by commanders/weapons operators, not AWS, and that where possible these decisions should be made in advance, when the weapons are deployed or even earlier. An interpretation of the way that IHL can be applied to AWS, detailing the information commanders require and the questions they should usually pose prior to and in the course of deployment. A description of real-world deployment scenarios, from simple to extremely complicated, looking at those elements of MHC standards that must be observed in order to be compliant with IHL norms. A restatement of the central nature of the constant care obligations and their implications for the precautionary principles of IHL, and how this works with AWS. A consideration of those scenarios during armed conflict in which human rights norms become more significant, and so more contemporary human decision-making and control is required, even in some cases demanding the shutdown of the AWS or a remote pilot taking over. It is important that in writing the above consideration should also be given to the ways in which rules may be applied differently depending on whether an armed conflict is international or non-international.

The sixth chapter would be concerned with accountability and responsibility, restating and applying regulations related to international criminal law responsibility for both individuals and commanders; this would encompass the responsibility of software programmers, manufacturers, and designers. This section could also be linked with chapter 5, clarifying what level of technical knowledge the capacity/limitations of a system a commander or weapons operator requires to make them the accountable person under IHL; this could also be extended to non-standard responsible bodies, e.g. procurement teams and legal review panels. This chapter would finally reiterate and detail the application of the generally agreed regulations regarding the responsibility of states in instances where the deployment of AWS has caused unlawful damage, injury, or death, even in instances where the damage could not be predicted or where a malfunction occurred.

The seventh chapter would deal with the law of neutrality, offering a restatement and application of the laws that ensure neutral states' territory remains inviolable in relation to AWS, and also detailing the rights and obligations of a neutral state regarding combatants that deploy AWS.

The final chapter would deal with the law of occupation and the restatement and reapplication of regulations applying to respecting, *inter alia*, protected property and persons within occupied territory, public order and safety, and the safety of the occupying authority. Because human rights norms play a greater part during occupations, this chapter might reiterate the necessity for attack parameters to be tightened, nonlethal operation to be considered, and/or simultaneous human control and/or judgment to be used for deployments in occupied territory. The above suggestions only represent a broad outline; however, they do make it clear that the potential exists to create quite a comprehensive AWS manual.
5. Conclusion

Reviewing the issues more closely, it is clear that this will not be a simple matter; in the past, IHL Manuals like Tallinn and AMW were created in relatively favourable political environments, whereas an AWS manual would not enjoy this luxury. NGOs are leading a campaign that is gathering support from certain states for the pre-emptive banning of AWS. This would mean that there would be significant political opposition to accepting permissive norms related to AWS in an IHL Manual. Because the stakeholders mentioned are in favour of an outright ban rather than normalizing AWS, this is obviously not the perfect environment for creating a broadly accepted Manual for AWS. Matters are not helped by the International Committee of the Red Cross (ICRC) having failed to commit to a position on AWS, and in fact having put forward concerns about them. This may demonstrate that the organization is reluctant to be a supporter of an AWS Manual, and this contrasts with past endeavours such as the San Remo Manual for naval warfare. In that instance, the ICRC was very supportive, which gave the San Remo Manual significant credibility due to the fact that the Red Cross is regarded as independent, neutral, and impartial and solely concerned with humanitarian issues. Thus, the apparent doubts about autonomous machines in warfare held by the ICRC may militate against wide acceptance of a Manual for AWS.

However, the ICRC has made no official statement calling for AWS to be banned. The Red Cross has taken an active role in research and in assembling conventions of technical experts on the relationship between humans and machines. These meetings have made a considerable contribution to the discussion regarding human control of weaponry, and they may demonstrate that the Red Cross is willing, albeit cautiously, to have some involvement with the development of a normative framework for the deployment of AWS.

Signed 74 years ago, it is clear that the Geneva Conventions are insufficient to regulate autonomous weapon systems at a time when artificial intelligence has not been discovered and it cannot be foreseen that weapons can destroy targets without human intervention. However, the CCW process in which autonomous weapons are discussed is slowing down due to the resistance of states. At the same time, many states have been investing in artificial intelligence technology and have an ambition to actively use autonomous weapon systems using artificial intelligence in their armies.

Although there is a growing consensus in the international arena that autonomous weapons systems cannot act in accordance with the fundamental principles of international humanitarian law and should be banned, banning them is not a viable solution and therefore limitations need to be imposed.

In order to minimise the negative effects of autonomous weapon systems, a consensus must be reached on the need for meaningful human control over the use of force during the CCW process. Although the CCW framework allows the establishment of rules that are applicable only in armed conflicts. The area of use of autonomous weapon systems includes law enforcement operations and counter-terrorism in addition to armed conflicts. Therefore, it may be advisable to develop a manual on autonomous weapon systems as they have great potential to allow flexibility since treaties are not comprehensive as manuals and in order to avoid political pressures. This article concludes that there may be alternative legal transplants for autonomous weapon systems based on the regulations in international humanitarian law regarding anti-personnel mines, cluster munitions, and incendiary weapons. This article offers a potential pathway in order to constitute an IHL manual on AWS which consists of eight chapters instead of banning AWS.
 Araştırma ve Yayın Etiği Beyanı
Bu çalışma için etik kurul onayı gerekli değildir.

Destek Beyanı
Bu çalışmanın finansmanı yoktur.

Çıkar Beyanı
Bu makalede herhangi bir çıkar çatışması bulunmamaktadır.
References


Human Rights and Conflict Resolution Clinic, Stanford Law School; NYU School of Law, Global Justice Clinic.


