

Section III: Remote and Autonomous Weapons



1. The technologies discussed in this Section are either novel or have yet to emerge and are not explicitly dealt with in either customary international law or in treaty law. The principal purpose of the present Section is to explain some of the main legal issues that the development of these new technologies seem likely to raise in relation to LOAC.
2. Different countries may choose to categorize these technologies in differing terms. This variety could not be adequately reflected in the present Section. Moreover, the terminology and definitions used in this Section may be expected to evolve in the light of future developments. Accordingly, the phrase “For the purposes of this Manual” (appearing in Rule 36 and other provisions of this Section) reflects the provisional status of the language that is employed.
3. The implementation of the law of targeting under LOAC is traditionally achieved by the human user of a weapon system applying the principle of distinction and the rules as to discrimination, proportionality and precautions. A number of the technologies discussed in the present Section may, in the future, enable a weapon system to make determinations as to whether an attack will take place and if so what the target will be and how the attack will be prosecuted. Even when the technologies covered by this Section are employed, the role of a human user of a weapon system may not be excluded. However, if no human being will play a role in the attack decision-making process, the question will arise as to whether some other method can be adopted to enable application of the principle of distinction and the rules pertaining to discrimination, proportionality and precautions. It was the position of the Group of Experts that, irrespective of the method of warfare adopted, the aforementioned principle and rules must be observed.
4. It should be emphasized that LOAC does not impose obligations on weapon systems themselves, but rather on the persons making decisions in connection with their use. In other words, LOAC requires that those persons will only act in compliance with LOAC principles and rules (taking into account the systems

capabilities and constraints). In the final analysis, legal responsibility will devolve on the State and on individuals involved in that activity (see Rules 43 and 44).

Rule 36

For the purposes of this Manual, a “remotely piloted aircraft” (RPA) is an aircraft that is controlled via a remote communication link by a human operator who is not located on board the aircraft.

Commentary

1. The term “remotely piloted aircraft” (RPA) has been used to reflect that the aircraft is piloted by an individual who is not on board. The word “drones” is also frequently used to refer to such vehicles. The controller of an RPA may occupy a control station distant from the RPA’s area of operation. From that control station the controller employs computerized links with the RPA to guide it and monitors the output of its sensors.
2. RPAs are aircraft and are distinguished from other aerial weapon systems such as missiles. In contrast to missiles, RPAs are normally recoverable.
3. The AMW Manual draws a distinction between “unmanned aerial vehicles” in general and “unmanned combat aerial vehicles”, the latter comprising unmanned military aircraft of any size that can carry and launch a weapon or that can use on-board technology to direct a weapon to a target.¹ The term RPA, however, does not distinguish between unmanned aircraft on the basis of their roles, which may include, e.g., reconnaissance, surveillance, information gathering, communications or other battle support, logistical or general military tasks and attacks.
4. RPAs can vary in size, e.g., from Global Hawk with a wingspan of 116 feet and a payload of up to 2000 pounds to the US Defense Advanced Research Projects Agency Nano Air Vehicle with a wingspan of 16 cm and a weight of 19 g. Both would, however, constitute aircraft,² and thus (if remotely controlled), RPAs.
5. RPAs using currently available technology, whether they are being employed on reconnaissance, surveillance, attack or other missions, are normally recovered at the conclusion of the assigned mission. However, the issue of recovery is not essential in terms of the definition of RPAs. The essential features of an RPA are that (i) it is piloted by a person who is not on board the aircraft and (ii) being an aircraft, it derives lift from the air. The possibility cannot be excluded that disposable RPAs may be developed. If such disposable systems derive lift from the air and are remotely piloted, they could, for the purposes of this Manual, be classed as RPAs.

¹*AMW Manual*, see fn. 1, rules 1(dd) and 1(ee).

²UK Ministry of Defence, *The Manual of the Law of Armed Conflict (UK Manual)*, Oxford: Oxford University Press (2004), paragraph 12.4.1 as amended.

6. During an international armed conflict, an RPA may only be used to exercise belligerent rights, such as attack or interception operations, if it fulfills the requirements of a military aircraft.³ To qualify as a military aircraft, it must be operated by the armed forces of a State, bear the military markings of that State (provided the size of the aircraft allows for such marking), be commanded by a member of the armed forces and be controlled by personnel subject to regular armed forces discipline.⁴

Rule 37

For the purposes of this Manual, a “highly automated” weapon system is a system that, once activated, is capable of identifying and engaging a target without further human input, while being constrained by algorithms that determine its responses by imposing rules of engagement and setting mission parameters which limit its ability to act independently.

Commentary

1. A “highly automated” weapon system performs functions in a self-contained and independent manner once activated. It independently verifies or detects a particular type of target and then fires or detonates a munition. Automated technologies in general are not new and have been employed in the past, e.g., in mines and booby-traps.⁵
2. Reference is being made here to “highly automated” as distinct from “automated” in recognition that there are numerous degrees of automation and a variety of functions that are capable of being automated. These may include, e.g., navigation of a platform; navigation of a munition; the co-ordination or fusion of data with a view to presentation of it to a pilot or other operator; functions associated with the fusing of the weapon, the locking on by an air to air missile to a target aircraft to which it has been directed by a pilot; and so on. Numerous weapon systems incorporate automated functions but do not come within the definition of autonomous systems, see Rule 38.

³Hague Rules Concerning the Control of Wireless Telegraphy in Time of War and Air Warfare (Hague Draft Rules of Aerial Warfare) (1923), *Laws of Armed Conflicts*, at page 315, Article 13; *UK Manual*, see fn. 2, para 12.34; German Federal Ministry of Defence, Law of Armed Conflict Manual (*German Manual*) (2013), Joint Service Regulation (ZDv) 15/2, para 1103; *US DoD Manual*, see chapter “Section II: Cyber Operations”, fn. 4, para 14.3.3.

⁴Hague Draft Rules of Aerial Warfare 1923, Articles 3, 13 and 16, see fn. 3; and *US DoD Manual*, see chapter “Section II: Cyber Operations”, fn. 4, paras 14.3.2 and 14.3.3; so, law enforcement, customs, or coastguard aircraft, including RPA, that do not qualify as military aircraft and that are not incorporated into the armed forces may not engage in hostilities. It remains to be seen whether, as small and unmanned military air platforms start to be more widely used, States continue to apply to them rules as to military and nationality marking.

⁵*US DoD Manual*, see chapter “Section II: Cyber Operations”, fn. 4, para 6.5.9.1.

Rule 38

For the purposes of this Manual, an “autonomous” weapon system is a weapon system that is programmed to apply human-like reasoning to determine whether an object or person is a target, whether it should be attacked, and if so, how and when.

Commentary

1. The concept of autonomy as used here may be narrower than that used by some roboticists.
2. There are different definitions of “autonomous weapon systems”. For example, the US Department of Defense Directive 3000.09 defines “autonomous weapon systems” as “a weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.” In this Manual systems described in the second sentence of the US definition come within the ambit of Rule 39 (b), *i.e.*, “man-on-the-loop systems”.
3. This Rule reflects that the single most important defining characteristic of an autonomous system is its ability to apply what perhaps can most accurately be described as “human-like reasoning”. By using this term, the Group of Experts was seeking to express the process of human judgment in which disparate facts are assessed and sometimes compared in order to reach an evaluative decision which will require the application of judgment. At the present time, such systems are not known to exist.
4. It is the application of human-like reasoning independently to identify and decide to engage targets that is the vital distinguishing feature of this technology. Such a weapon system is not pre-programmed to target a specified object or person. It is the software that decides which target to engage, how and when. Accordingly, the weapon system is making the relevant judgments by applying the kinds of thought process that a human being would use when employing a more conventional weapon system, and, again like a human decision-maker, the autonomous weapon system has the capacity to adapt its behaviour in response to changed circumstances.
5. The reference to being “programmed” in the definition indicates that the system’s software will have been so engineered as to enable, perhaps require, the system to analyze information and make decisions having applied human-like reasoning to the facts that either it detects or that are otherwise disclosed to the system. The reasoning process is likely to be similar, in terms of decisions made, to that which a human being might be expected to undertake, although the logical processes may not necessarily be the same as a human being would apply.

6. While it is possible to characterize an autonomous weapon system as making a decision in a factual sense, it is also critical to emphasize that LOAC imposes obligations on persons and does not impose direct obligations on the weapons themselves. LOAC does not, for example, express a requirement that an autonomous weapon system must determine whether its target is a military objective, if no human being is involved in the attack decision-making process. Nevertheless, LOAC still requires the attack to be conducted in accordance with targeting law (see Rule 41). For State responsibility and any responsibility by individuals involved in an attack, see Rules 43 and 44.

Rule 39

For the purposes of this Manual:

- (a) **A “man-in-the-loop system” positions the operator within the loop formed by the decision-making process of the system such that the human operator decides on the firing of a weapon.**

Commentary

1. The cycle of receiving input, analyzing the input and taking action can be regarded as a loop, and the presence of the human controller within this loop characterizes the system as “man-in-the-loop”. A “man-in-the-loop system” positions the operator within the loop formed by the decision-making process of the system, using up- and down-links to the remotely piloted aircraft.
2. Up- and down-links are the means whereby the human operator communicates with the vehicle and whereby the operator receives communications from the vehicle.
3. Where RPAs are concerned, the link from the controller to the RPA (see Rule 36) is used, *inter alia*, to direct the flight of the RPA and to instruct the RPA to perform tasks. The link down from the RPA to the control station is used, *inter alia*, to deliver information from on-board sensors. Taken together, these links can be regarded as a loop, and the presence of the controller within this loop characterizes such systems as “man-in-the-loop systems”.
4. Remotely controlled vehicles in other environments may have similar capabilities for the receipt and transmission of data.

- (b) **A “man-on-the-loop system” is one that is capable of highly automated or autonomous operation but is supervised by a human operator who has the capability to intervene and override a decision, such as the decision to fire a weapon.**

Commentary

1. A “man-on-the-loop system” is differently configured from a “man-in-the-loop system”. The operator is not positioned, either physically or structurally, within the loop formed by the system’s decision-making process to fire a weapon after receiving external inputs. The weapon system may be capable of making and

implementing its own determinations as to attack, reconnaissance, information gathering or other tasks, but the “man-on-the-loop” element inserts the presence of a human operator who—while not involved in the firing of the weapon or other decisions—is nevertheless able to observe the determination being made and the action being taken by the weapon system and to intervene and countermand any determination or actions that seems likely to lead to unlawful or undesirable consequences. Such aircraft can be distinguished from other aircraft in which the human controller decides which target is to be engaged or which task is to be undertaken and who undertakes the attack by initiating the firing mechanism or transmitting the instructions for the performance of the chosen task using the remote-control facility built into the RPA system.

2. The use of a “man-on-the-loop system” for the gathering of information, for reconnaissance or similar tasks, could assist in addressing issues under the law of targeting. Indeed, using such systems to obtain timely, accurate information as to the situation in an area where attacks are intended is likely to promote adherence to the principle of distinction. There is no LOAC rule prohibiting or limiting the use of such technologies. Furthermore, such systems will generally be equipped with sensors and associated systems that are designed to allow military commanders to control the effects of these weapons (e.g., to ensure that the weapons do not cause excessive collateral damage or result in “friendly fire”).
3. The human being who is monitoring a “man-on-the-loop” system and who is able to cancel a firing determination that the system might undertake, may assist in ensuring that the system can be used in accordance with LOAC. This is not intended to imply that LOAC requires that a person must necessarily be in or on the loop to render the use of a highly automated or autonomous system lawful. If the highly automated or autonomous system is capable of being used in accordance with targeting law, LOAC contains no specific requirement that a person be either in or on the loop in the sense that those terms are employed in this Manual. Rather, where necessary, the monitoring can be conducive to avoiding or minimizing the risk of civilian casualties.
4. The person “on-the-loop” may find it necessary to intervene and countermand any determination made by the weapon system for a variety of reasons. So, for example, there could be clear cases in which (if the weapon were to fire) a civilian taking no direct part in the hostilities, or a civilian object, would be struck, and the “man-on-the-loop” would be obliged to intervene and stop the weapon system.⁶ There are other circumstances when such intervention would be called for, for example if the object of attack is a person or object entitled to special protection under the law of armed conflict, or if the attack that the weapon system has decided upon would be contrary to the commander’s intent.

⁶AP/I, see chapter “Section I: Outer Space”, fn. 13, Articles 51(2), 52(1) and 57(2)(b).

5. While the presence of the person “on-the-loop” may, in the context of a particular weapon system, be the aspect that enables the required precautions in attack to be undertaken, the circumstances in which the person is operating “on-the-loop” will determine whether the precautions are actually taken with sufficient care. Thus, for example, if a person is contemporaneously placed “on-the-loop” of numerous weapon systems, or of weapon systems undertaking numerous contemporaneous operations or attacks so that he/she is not practically able to monitor properly the precautions that targeting law requires (including those referred to in the present Commentary) this might have the consequence that the requirement to take feasible precautions would not be complied with to an acceptable degree. The word “might” is used here because there may be other elements of the weapon system or of its method of operation that do enable particular precautions to be taken. The point remains, however, that if legal compliance relies on a man “on-the-loop” and if that person is over-tasked in whatever way, compliance is put at risk.

Rule 40

For the purposes of this Manual, a “swarm” is a group of aircraft or other vehicles of any size that is performing (or is intended to perform) military tasks in which the individual aircraft or other vehicles are autonomously coordinating or acting in formation.

Commentary

1. Given the early state of “swarming” technology, it is unclear what could arise in the context of aircraft being operated as part of a “swarm” for the performance of military tasks. Swarms could comprise numerous aircraft and whether the individual vehicles of the swarm are large or small or of various sizes might not be relevant to the characterization of the group as a swarm. It is possible that some swarms will operate such that the individual members maintain a fixed formation while other swarms may involve dissimilar movements. Swarms could involve RPAs, highly automated systems or autonomous systems. Other swarms may comprise a mixture of these types of platforms, or the same platforms may have different modes of operation.
2. Whether operating in formation or with the individual vehicles undertaking dissimilar movements, the swarm will need to maintain some form of coordination among its vehicles to avoid collisions and other mutual interference.
3. What appears distinctive regarding “swarms” is the use of autonomy to coordinate vehicles in the swarm by, for example, distributing tasks among vehicles in the swarm.

Rule 41

The employment of remotely piloted, highly automated or autonomous systems and swarms for the purposes of attack is subject to the applicable

principles and rules of LOAC, in particular distinction, proportionality and the obligation to take feasible precautions.

Commentary

1. The Group of Experts agreed that the existing principles and rules of LOAC are the basis on which the lawfulness of using RPAs, highly automated or autonomous weapon systems, or swarms is to be judged.
2. For the notion of “applicable principles and rules of LOAC”, see paragraph 4 of the Commentary to Rule 2.
3. Human-like reasoning (referred to in Rule 38) may not be necessary to secure compliance with targeting law by an autonomous weapon system in specific circumstances. For instance, the employment of a weapon system may be limited to a time and location where all those present certainly qualify as lawful targets.
4. In other situations, it would be necessary to ensure that the introduction of an autonomous weapon system operating with human-like reasoning would be in full compliance with the principles and rules of LOAC. This could be attained if the weapon system were able to make two classes of determination. The first concerns the lawfulness of the target, *i.e.* a determination whether it is a combatant, a civilian taking a direct part in the hostilities or an object that is a military objective. The second concerns the legality of attacking it in the circumstances prevailing at the time.
5. It should be stressed that RPAs, autonomous weapons systems and “swarms” are not per se prohibited by the principles and rules of LOAC.
6. If a swarm is used to undertake reconnaissance, information gathering or other tasks that do not constitute part of an attack, LOAC issues will not be engaged merely by virtue of the character of the group of aircraft so involved as a swarm.
7. If a swarm is being used to undertake attacks, the factors that determine whether and to what extent controllers or operators are required may include: (i) the number of aircraft in the swarm; (ii) the number, nature and circumstances of the targets that are to be attacked; (iii) the nature, quality and reliability of the up- and down-links to each aircraft; and (iv) the degree to which the swarm is operated in a formation.
8. If achieving compliance with the applicable principles and rules of LOAC necessitates human presence “in” or “on-the-loop”, it is important to ensure that the relevant personnel are not tasked to such a degree or located in such a way as to preclude their proper performance of the required feasible precautions. If the technology incorporated into the swarm is such that the individual weapon systems are capable of making the determinations required by targeting law in the intended circumstances of use, the presence of a person or persons “in” or “on the loop” of elements of the swarm may not be required. It will be a question of fact whether the swarm does indeed have that technical capability and whether it is able to operate with an acceptable level of reliability. In certain circumstances,

achieving compliance with targeting law may require that there be sufficient controllers or operators adequately linked in with the activities of each aircraft.

9. The determination whether or not to act in formation may be taken autonomously.

Rule 42

- (a) **In the study, development, acquisition or adoption of new weapon systems addressed in this Section, a State that is party to Additional Protocol I must determine whether its employment would, in some or all circumstances, be prohibited by any rule of international law applicable to that State.**
- (b) **In the acquisition of a new weapon system addressed in this Section, a State that is not party to Additional Protocol I should determine whether its employment would, in some or all circumstances, be prohibited by applicable principles and rules of LOAC.**

Commentary

1. For the interpretation of this Rule, see the Commentary on Rule 7 which is applicable *mutatis mutandis*.
2. There are at present no rules of LOAC that specifically refer to RPAs or other remotely piloted or controlled weapon platforms. Similarly, no specific rules refer to highly automated or autonomous attack technologies as such.⁷ The fact that a weapon system is remotely controlled, highly automated or autonomous does not, therefore, *per se* render the system unlawful.
3. When the review concerns such weapon systems, it is necessary for the person conducting the weapon review to determine whether the weapon system is capable of being used in accordance with the rules prescribed by LOAC. The question is not whether the weapon system will comply with targeting law on a particular occasion but whether the way in which the system is designed and will be operated enables the targeting law rules to be properly applied. In practice, the main question may be whether the anticipated employment of the weapon system will be consistent with the principles of distinction and proportionality.

Rule 43

With respect to an armed conflict, States bear responsibility for internationally wrongful operations using RPAs, highly automated weapon systems or autonomous weapons that are attributable to them. Such responsibility encompasses actions by all persons belonging to the armed forces.

⁷Note, however, that Protocol (II) to the Conventional Weapons Convention on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II to CCW) (1980), *The Laws of Armed Conflicts*, page 185, address, inter alia, “other devices” which include manually emplaced munitions actuated by remote control.

Commentary

1. For an interpretation of this Rule, see the commentaries on Rules 5 and 21.

Rule 44

All those involved in the conduct of operations, including attacks, using RPAs, highly automated weapon systems or autonomous weapons, are responsible for their respective roles and, commensurate with their involvement, have obligations to ensure that such operations are conducted in accordance with the applicable principles and rules of LOAC.

Commentary

1. See Commentary on Rules 5 and 22.
2. Numerous individuals may have various roles that may be relevant to the conduct of an RPA operation. Those individuals include, but are not limited to: (i) the RPA operator; (ii) any technicians who may be assisting the operator; (iii) those involved in launching the RPA; (iv) the commander of the mission; (v) those who planned the mission; (vi) those who prepared the software; (vii) those who loaded data into the mission control systems; (viii) those who gave legal advice in connection with the mission and so on. All such individuals have obligations with respect to the implementation of applicable principles and rules of LOAC.
3. The degree and nature of the responsibility of each individual depends, *inter alia*, on the nature and extent of that individual's role, on the rank of the individual, on the operational relationships between the persons involved, and on the information available to the particular individual at a specific time. Although the negligent performance of duties is likely to attract disciplinary liability for armed forces members under their service code, gross negligence, recklessness and intent may, depending on the consequences, involve criminal liability.
4. Manning and other arrangements for RPA operations should facilitate compliance with targeting law.
5. The information that the sensors aboard an RPA gather may be used to support the decision to engage a specific target, may be used in support of other military operations or may contribute more generally to the commander's picture of the battlespace. An RPA that is on a reconnaissance or information gathering mission will generally be used to provide information for one or more of these purposes.
6. The mere fact that an autonomous or highly automated weapon system is used to undertake an attack does not preclude the potential liability under international criminal law of any person for his/her involvement in such a military operation.

7. In view of the novelty and complexity of the technology, it is not clear exactly where responsibility under international criminal law will lie for specific acts performed by an autonomous or highly automated weapon system. See chapter “Section XVII: International Criminal Law” with regard to individual criminal liability in international law and command responsibility particularly.

Rule 45

A person who wrests control of a weapon system referred to in this Section assumes responsibility for its subsequent use in accordance with the degree and the duration of the control exercised.

Commentary

1. This Rule refers to the individual responsibility of a person who wrests control of weapon systems referred to in this Section. Should such a person act on behalf of a State, his/her wrongful act will be attributable to that State which will bear State responsibility, see Rule 43.
2. This Rule reflects that a cyber hacker who achieves control of the enemy’s weapon system or its munition becomes responsible for his/her subsequent employment of the weapon. The hacker’s employment of the weapon must comply with principles and rules of LOAC including distinction, discrimination⁸ and proportionality as well as the obligation to take precautions in attack. If the cyber hacker does not achieve absolute control of the weapon system and its munitions, but interferes in the way in which the weapon system and munitions are operated by the enemy, responsibility for the use of the weapon system or munition should be determined in accordance with the following criteria.
 - a. If a cyber hacker exercises control of a weapon system referred to in this Section and knowingly or intentionally directs its weapon—or knowingly or intentionally causes the weapon system to direct weapons—at a target or category of targets of his/her choice, he/she becomes responsible for the consequences of such employment of the weapon.
 - b. This subparagraph applies if the cyber hacker does this with the intention of causing the weapon to attack civilians, civilian objects or persons or objects entitled to specific protection, or to undertake indiscriminate attacks. If this sub-paragraph applies, the cyber hacker is responsible for the consequences of the use of the weapon.
 - c. If in the circumstances described in sub-paragraph b the cyber operation foreseeably causes the adverse party’s attack(s) to become indiscriminate,

⁸Discrimination is here used to refer to indiscriminate attacks.

the cyber operation is likely (depending on the circumstances) to conflict with obligations under Articles 57(1) and 58(c) of APII.⁹

3. If two adversaries are contesting control over a weapon system and the system ends up crashing and harming civilians, responsibility may be impossible to attribute to either of them.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.



⁹See chapter “Section I: Outer Space”, fn. 13.