Polish Political Science Yearbook vol. 46 (2) (2017), pp. 205–223
DOI: 10.15804/ppsy2017213 PL ISSN 0208-7375

Eric Pomès
Catholic University of the Vendée – ICES (France)

Technological Innovations and International Humanitarian Law:
Challenges and Tensions

Abstract: In recent years, armed conflicts have changed in nature (civil war, 'terrorism') and the means used are increasingly technological (robotization, cyber war). Faced with these developments, some would claim International Humanitarian Law (IHL) is outdated. While these technological innovations present new challenges in the application of IHL, it still constitutes a relevant legal framework for armed conflicts and the conduct of hostilities. Indeed, the flexibility of IHL allows it to adapt to contemporary conflicts. Therefore, this shows that the statements about its obsolescence are primarily political in nature.

Keywords: *cyber war, drones, military robotization, international humanitarian law, principle of distinction, proportionality, precautions in attack.*

Introduction

Today, armed conflict no longer consists of two regular armies opposing each other on a broad plain. Armed conflict takes place in areas which are densely populated or difficult to gain access to. Armed conflict arises either between non-state actors, or between a non-state group and a conventional army. This new reality influences the application of international humanitarian law in different ways (Crawford, 2016; Kaldor, 2012). When can it be said that there is an 'armed conflict' – which there needs to be if international humanitarian law is to be implemented? How can we describe the people who participate in such hostilities? How should we protect civilians considered by non-state actors to be human shields?

The blurring of the boundaries on the battlefield is the second major change. Contemporary weapons have increased the distance between the attacker and the target; the battlefield seems to be everywhere. Again many questions arise: can we use military force anywhere? Do these new means of combat discriminate between combatants and civilians? Some of these issues have already been raised in the 1990s. Indeed, the proliferation of non-international armed conflicts with an ethnic nature suggested that international humanitarian law was no longer adapted to the 'new forms of war'. Since the early 2000s, international humanitarian law has faced new challenges: the war on terrorism, cyber warfare, and robotization of the battlefield. Targeted killing by drones, and suspicions of cyberattacks from Russia show the importance of the use of new means and method of combat. Despite the importance of the challenges posed by terrorism, the rest of the article will focus on the difficulties arising from robotics and cyber war. These new means and methods of combat inevitably influence how to wage war and create challenges to IHL. In fact, they could lead to developments such that IHL cannot effectively regulate their use.

The history of wars has been marked by the technological progress of armaments (Van Creveld, 1991). Armament innovations (nuclear weapons, chemical weapons, etc.) have always questioned the relevance of the existing rules and the need to create new ones to govern them (see for *example Geneva Protocol on Asphyxiating or Poisonous Gases, and of Bacteriological Methods* – 1925 –, *Convention on the Prohibition of Biological Weapons* – 1972 –, – Gill, 2016). The contemporary era does not escape this reality. These technological developments will affect the manner in which armed conflicts are and will be conducted (Bousquet, 2011; Stewart, 2009). However, while previously new weapons have tended to strengthen destructive capabilities, the problem of robotization in general and LAWS in particular is of a different nature. This new generation of weapons, taking advantage of computer advances allows on the one hand, a geographical and therefore physical distance between the target and the military personnel using the weapon and on the other hand, the means to gradually exclude man from the process of their use. While innovation in weapon technology is as old as warfare itself, the rise of new weapon technologies like cyberwarfare, military robotization, and in particular autonomous weapons have raised fundamental questions about the impact of IHL on the battlefields in the future.

The first problem is to determine whether or not there is an 'armed conflict'. This question is not new. The difference between the past and now, perhaps, is that the adversary, or even the attack, cannot be seen. It is therefore difficult to ascribe legal status to certain situations. The second difficulty concerns the principle of distinction and the principle of proportionality. It is difficult to identify and distinguish between civilians and combatants, the choice of targets, etc. These issues have

been accentuated by the recent developments, and have perhaps even lead to the problem becoming systematic. Finally, as with any technological developments in weaponry, we have to ask whether robots or cybernetic weapons respect the principle of humanity. Indeed, even if the need to protect soldiers from harm will always be an overriding factor for any military and new weapon technologies, the belligerents will not have an unlimited choice in the means of warfare (see article 35 API). This question is urgent because of the development of lethal autonomous weapon systems (LAWS). These systems will mean that human beings will no longer participate in the use of armed force.

Therefore, the question is whether military robots and cyber-weapons, by reducing the role and the control of human beings when using force, makes the existing IHL obsolete. The thesis defended in this article is that despite the tensions on the principles of IHL and the risk of blurring these principles, the emergence of these new means of combat does not necessarily require an evolution of IHL. The existing rules are sufficiently adaptable to frame these new weapons. This article explores the way in which those rules may be interpreted, adapted and applied in the technological evolution context.

The real danger for IHL is the impact of ideological interpretations which distort the law. So the question raised by the technological evolutions dealt with in this article is if there is a need to create a new arms control regime; in other words, a governance of cyber-weapon, a governance of military robotics because the question of the lawfulness *per se* of these weapons (this issue will not be discussed in this article) should be distinguished from the question of the legality of their use.

To answer these questions this work is divided into four major sections. The first section examines the influence of these new challenges in determining the existence of an armed conflict. In the second section the difficulties in applying the principle of distinction in the use of these new means of combat is discussed. Their influence on the principle of proportionality is outlined in the third section. The last section tackles the perspectives on the regulation of these new means of combat.

The Complexity of the Application of IHL in View of New Challenges: Determining the Existence of an Armed Conflict

The proliferation of military robots, in particular the targeted killing operations carried out by drones and the use of cyber-weapons, allow the multiplication of more or less hostile operations of the states without the deployment of military forces on the ground. If the bombing of the villa of a terrorist leader in a country by a drone or the use of a virus against industrial installations in another country may be considered

like unlawful unfriendly acts, the question is whether these acts can bring an armed conflict into existence.

Categorizing a situation as an 'armed conflict' is important because the IHL will be able to regulate the hostilities and it enables to override some of the peacetime rules of international law. Thus its existence permits the use of military force, of destruction, and of detention, etc. Even though there is no definition of 'armed conflict' in international law treaties, it is understood to be 'the use of armed force between two belligerents' (ICTY, Dusko Tadic, Decision on the defence motion for interlocutory appeal on jurisdiction, IT-94–1-A, 2 October 1995, para. 70). The question of qualification can be approached in two ways. Thus, a broad vision of qualifying conditions can be used to facilitate the application of IHL. Conversely, adopting a restricted vision will apply a higher level of rights and duties to better protect individuals by applying peacetime law. Finally, under international humanitarian law five categories of armed conflicts can be distinguished (see Wilmshurst, 2012): declared hostilities between two states; undeclared hostilities between two states; an international armed conflict between the government and a national liberation movement; a non-international armed conflict between a state and non-state armed groups; and a non-international armed conflict between non-state armed groups.

Robots and cybernetics as new methods and means of combat question the existence of an international conflict in three ways. First, they raise the question of whether their use can be described as an armed force. Bombing and the deployment of troops are clearly seen to be the use of force. Therefore, when robots are used to bomb for example in another state, this should be considered to be the use of armed force. This is more complex in the case of the use of cyber weapons because of the lack of physically destroying or damaging military or civilian infrastructure (kinetic effects). For some scholars the lack of kinetic effects implies that cyber-attacks cannot bring an armed conflict into existence. However, this reasoning is not very convincing because it leads to recognize the existence of an armed conflict when a State bombs a house but not in case of a cyber-attack on critical infrastructure (such water or electricity networks) without kinetic effects even if it negatively affects people's lives. In fact, there is nothing to prevent a cyber-attack being characterized as an armed conflict because the term 'armed' involves dynamic acts producing violent, destructive results (Boothby, 2014). In other words, there is armed conflict when the actions of a state are considered to be unacceptable coercive measures by the victim state. Furthermore, it doesn't matter that one of the belligerents denies the existence of an armed conflict, or the place of hostilities or the forces involved because the determination of the existence of an armed conflict within the meaning of Article 2 (1) must be based solely on the prevailing facts demonstrating the *de*

facto existence of hostilities between the belligerents (ICTY, Boškoski and Tarčulovski Trial Judgment, 2008, para. 174)

Secondly, the common difficulty for the classification of armed conflict is whether a certain threshold of intensity is necessary for the application of rules of IHL. Although no clear position is taken by scholars, the majority consider that no threshold condition is required for a situation to be classified as an 'international armed conflict' (ICTY, Delalić Trial Judgment, 1998, para. 184). The existence of an armed conflict will be deduced from the facts. The existence of an armed conflict therefore depends on objective criteria (International Law Association, 2010, p. 33). There will be international armed conflict whenever a state commits an armed hostile act against another state. However, the state practice and some scholars suggest in the case of isolated or sporadic inter-state use of armed force that such situations would not qualify as international armed conflicts because of their short duration or the low intensity of the violence involved (Greenwood, 2008, p. 48). This latter position is important in the context of the use of robots and cyber operations (Lemieux, 2015). Indeed, when cyber activities and robots are used by one state against another in conjunction with and in support of more classic military operations, 'there is no doubt that such a situation would amount to an international armed conflict' (ICRC, 2016 para. 241). However, the situation appears less obvious when cyber operations and robots are the only means by which hostile actions are undertaken and when these operations remain isolated acts. Could these sporadic, isolated actions be considered as a resort to armed force under Article 2 (1)? Would the threshold of harm tolerated by states affected by these actions be different depending on the nature of the target, of the aim of the act?

These new means of combat complicate the characterization of armed conflict, not in themselves but because they enable to multiply actions of low intensity against or within a state. Therefore, to know whether IHL applies to their use is not a problem of rule but of interpretation of them. To this end, it is possible to apply the Michael J. Glennon's pragmatic view of international law (Glennon, 2010). Thus, if global peace and security and the protection of individuals are the main policy objectives then the vision rejecting the application of IHL should be preferred as it will apply the peace-time rules of international law. If the major objective is either to derogate from the rules of peacetime or to regulate hostilities, then the exclusively objective approach should be adopted.

A third option could also be adopted. The low intensity, the isolated nature of robotic or cybernetic operations could lead to the suggestion of adding a condition to demonstrate the existence of an international armed conflict: the animus belligerenti. Moreover, state practice seems to adopt this approach implicitly since states do not support the application of IHL in isolated or low-intensity operations.

Thirdly, the use of robots and cyber weapons makes it more complicated to prove the involvement of a state in an operation. Yet, there can be armed conflict only if one state attacks another. The use of these means of combat complicates the attribution of the operations because the perpetrators can the origin of the attack. For example, backtracking a cyber action becomes far more difficult when it involves an international border. Attackers will almost always route their attacks through servers in several countries, launch cyber-attack in an indirect fashion (use the enemy's resources against them, by seizing control over computers in the target nation and launching the attack from within the victim's borders or use non-state actor) (Lin, 2012). This complexity of the technical assignment impacts the attribution in the legal sense (who is responsible for the wrongful act)[1]. Without proof of origin of the attack, the victim state will be unlikely to prove that it is a case of international armed conflict.

Another difficulty is that these means of combat are not necessarily used against a state but against non-state actors (terrorists, etc.). Does IHL apply to these situations? Two different texts can be applied to these situations. First, common Article 3 of the four 1949 Geneva Conventions which would apply 'In cases of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties'. The application of IHL depends on the identity and degree of organization of the parties and the intensity of the conflict. Secondly, the 1977 *Additional Protocol II* (APII) applies to 'all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions … and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol'. In our hypothesis, the application of this text must be rejected because it concerns hostilities between groups, which does not necessarily control a territory, and a state but in the territory of another state. The question is therefore whether common Article 3 of the four Geneva Conventions applies, for example, to the US targeted killing operations in Yemen. If the condition of identity and organization of the parties is fulfilled, the intensity condition is not satisfied. Indeed, these operations are not continuous but isolated. Therefore, it is the right of peacetime, including human rights, that should apply.

Another hypothesis can be envisaged: the attack, for example a cyber-attack, of a state by a non-state actor. In this case, only common article 3 could possibly apply. However, classify a simple cyber-attack as a 'non-international armed conflict' will be very difficult because it is not certain that the groups using cyber-attacks are necessarily

[1] See the International Law Commission's Draft Articles on State Responsibility.

organized (e.g. Anonymous) (Geiß, 2013). In view of the intensity condition, only cyber-attacks producing the most violent consequences could be regarded as 'non-international armed conflict'. But above all the hostilities are, in this case, isolated.

Once again the application of IHL will depend on the interests involved. If the interest is either to derogate from the rules on the use of force in peacetime or to frame the hostilities, then the IHL can be applied widely. If, on the contrary, the aim is to limit the use of armed force, then a restrictive application must be adopted. To conclude, the majority of the states would want to apply the rights allowed by IHL, but without the protections provided by it. As soon as these means of combat are used 'in the context' of an armed conflict, the IHL is applicable and thus applies to the operations. The next section looks at the challenges of these new means of combat under the principles guiding the conduct of hostilities; in particular the principle of distinction.

Challenges Blurring the Principle of Distinction

The principle of distinction is found in the preamble of the St Petersburg Declaration 1868 which states that war is to be waged against the enemy's armed forces, not against its civilian population. Attacks are to be directed at military targets only. So, under the rule of distinction, a distinction should be made between combatants and civilians at all times and in all places (see articles 48 and 51–2–*Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*–Protocol I–, 8 June 1977–API). This distinction is very complex to implement in contemporary conflicts. Then how are the participants in hostilities determined?

The term 'combatant', in the sense of the 1949 Geneva Conventions, identifies persons who have the right to participate in hostilities (members of the armed forces, etc.). The combatants can thus be targeted by a drone, for example, at any time and any place. However, in contemporary conflicts either this status does not apply (Non International Armed Conflict) or those who participate in hostilities have no right to do so (civilians participating directly in hostilities). The introduction of LAWSs will be lawful only if they are able to distinguish all persons who do not enjoy protection from direct attacks on civilians, ie., combatants within the meaning of the Geneva Conventions and those participating in hostilities without authorization (members of non-state armed groups and civilians who directly participate in hostilities). This latter group is comprised of two categories of people. Firstly, the members of non-state armed groups who are engaged in a continuous combat function, *i.e.* preparing, executing or controlling the acts or transactions constituting a direct participation in

hostilities. Secondly, civilians directly participating in hostilities (defence contractor employees etc.) meaning civilians committing a hostile act causing injury (causation must be direct) to one of the conflicting parties with the intention (belligerent nexus) to promote one party at the expense of the other. These civilians lose their immunity against direct attack for the period of their participation (Melzer, 2009).

Questions of distinction do not really arise for current robots because a person is always in the loop but they will do so for autonomous weapons systems (Bhuta, Beck, Geiß, Liu, & Kreβ, 2016). These robotic weapons systems, once activated, can select and attack targets without further intervention of a human operator (Boothby, 2013, p. 51). How can these autonomous systems distinguish between combatants and non-combatants? The distinction of combatants in an IAC should not pose any real difficulties on the condition that the LAWSs are able to recognize the uniforms and to distinguish the soldiers protected by immunity from attacks (chaplains, sanitary auxiliaries and non-combatants – wounded). The distinction between individuals directly involved in hostilities will certainly be more complex. Indeed, LAWSs must be able to distinguish between civilians on the one hand and members of non-state armed groups on the other, provided that they perform a continuous combat function, ie., prepare, execute or actions or operations that constitute direct participation in hostilities, as well as civilians directly involved in hostilities (private military company's employees, etc.) understood as civilians committing a hostile act causing injury (causality must be direct) to one of the Parties to the conflict with the intention (belligerent nexus) to favor one of the parties to the detriment of the other. These civilians then lose their immunity from direct attacks for the time of this participation. This inevitably raises the question of how LAWSs will determine their target. Two methods seem possible. In the first, it is a military leader who designates its target by coordinates, by the introduction into the system of a face, etc. In the second, the LAWS will determine or treat the target without human intervention. Only this last hypothesis will be discussed. This method asks the question of what criteria will be used to decide an attack. The first criterion could be databases. LAWS will decide an attack once it recognizes a target identified as a combatant in one of its databases. The legality of such a process will require at least daily or even real-time updates to these bases to take account of possible changes in the status of individuals, such as the departure of an armed group. So it will not be the LAWS that will really determine the target, but the military leader, from information that it will pass on to the LAWS via the updates. The LAWS would therefore be autonomous during the execution of the attack but not in the choice of the target. Action based on a database that recognizes distinctive signs and faces, however, appears to be a solution applicable only to combatants and members of armed groups with a continuous combat function. Such

a method seems difficult to apply to civilians directly involved in hostilities, since their targeting requires verification of the meeting of certain conditions (belligerent nexus etc.) at the time of the attack. Thus, in these cases, LAWS could only treat the target if it was at the time of the attack in a phase of participation in hostilities. Otherwise, the individual is protected as a civilian.

Faced with these difficulties, LAWS could determine its target according to another method: the activity of a person. The LAWS would decide an attack if an individual behaves in a hostile manner. The attack would then find its trigger in the position, weapon or threatening activity of that individual. This position would limit the hypotheses in which members of non-state armed groups and civilians directly involved in hostilities could be targeted, thus respecting a restrictive interpretation of targeting that is more respectful of the right to life. However, how to qualify an act of hostile? The whole difficulty lies in the definition in computer terms of the term 'threat or hostile act'. The wearing of a weapon may be considered hostile, but this does not automatically mean that its holder can be legitimately targeted.

Similar difficulties arise in cyber warfare because the direct participation of civilians in cyber operations will be greater than in traditional military operations. If the civilian belongs to a state or to a military non-state actor, he will lose his protection against attack only when he will participate directly to the hostilities and has a continuous combat function. The problem is to determinate what is a continuous combat function in the context of cyber military operation. A person executing a cyberattack against UAV control systems, for example, will certainly be regarded as have a continuing combat function because his acts will affect the capacities of the enemy. But this is less certain for a person who simply creates a virus without participating in the operation.

Similarly, it is complicated to determine the status of a civilian who participates directly in the hostilities, for example launching a cyber-attack against one of the parties to the conflict. There is a debate amongst scholars as to the necessary degree of damage for such a determination to be made (Allan, 2013). For the ICRC, it is necessary for the act to cause physical or material damage (Melzer, 2009, p. 46). However, for the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, there is direct participation in hostilities as soon as the act adversely affects the opposing military operations. This difference illustrates perfectly that interpretation is subject to the interests of the interpreter of the rule. The ICRC's interpretation is intended to limit the loss of protection against attacks, whereas the purpose of the interpretation of the *Tallinn Manual*, which is fairly close to American interests, is to facilitate the loss of such protection.

Moreover, the ICRC requires there to be a link between the act and the damage, whereas the *Tallinn Manual* merely requires an intention (Schmitt, 2013, p. 119).

The challenge will be to determine whether an individual who designs viruses may be considered as a direct participant in hostilities. Once again the two interpretations are explained by the aims pursued. The way followed by the *Tallinn Manual* seems too permissive. It would allow targeting anyone who had participated in the operation in one way or another, contrary to the objective of IHL.

Finally, there is also a debate on the belligerent nexus. For the ICRC it is enough to support one party against the other (Melzer, 2009, p. 58). According to the *Tallinn Manual*, the act must be directly related to hostilities (Schmitt, 2013, p. 119). Therefore, depending on the interpretation of the definition, a hacker could be regarded as a civilian directly participating in hostilities if his action undermines military operations, or as a simple civilian if his act does not support any belligerent. Similarly, the creator of a virus will be regarded as a simple civilian if his role is limited to providing the cyber weapon. He will be a civilian directly participating in hostilities if he works on the virus during the attack.

The principle of distinction also applies to the objects[2]. Under IHL, two types of objectives that can be targeted must be distinguished. Firstly, there are military objectives by nature. These are objectives which, because of their characteristics, are permanent military targets such as military bases, etc. Secondly, there are military objectives by use: these are civilian objects becoming military objectives. For this, two conditions must be fulfilled: the object constituting the objective must contribute to the military action of the adversary because of their location, purpose or use and its destruction must offer a military advantage to the attacker.

For any attack the military character of the object must be identified. This determination is problematic in the context of cyber war because the entire infrastructure (servers etc.) consists of dual-use object (Geiß & Lahmann, 2012). Such infrastructure is used for both military and civilian purposes. So it is important for military leaders to determine the object of the attack precisely. This obligation must be taken into account when designing cyber-weapons in order to limit their effects to the targets without spreading beyond them without discrimination. For example, during the attack of the Iranian nuclear power plant by the Stuxnet virus, the objective was not the Siemens software but the centrifuges.

[2] Article 52 (2) AP I provides that: "Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage".

The current robots pose no particular problem concerning the issue of the determination of military objectives, because targets are chosen by the military leaders. The appearance of LAWS does however raise the question of the identification process. As with any attack, the use of LAWSs will require the military character of the objective to be determined. Hence the important question of the identification process. The most obvious is the use of a database. This would integrate the identification of military equipment (tank …), coordinates (staffs) and so on. In these cases, respect for the principle of distinction does not appear to be difficult. On the other hand, the identification of military objectives by use seems more complex. If the object is targeted by a database or if the object is the target of the operation, the conclusions are the same as those made with regard to the qualification of individuals; the LAWS will not make a choice, it will execute the order given by the military leader. Assuming an attack using coordinate programming, the use of LAWS does not change what already exists since the entire qualification operation was carried out before the programming. More complex is the hypothesis in which the LAWS would decide to attack a civilian object which it considers a military objective within the meaning of Article 52 (2) of the API. The difficulty here is the need to make a judgment to determine the military character of the objective. Indeed, a civilian object becomes a military objective provided that it has a strategic value – the term by destination, for example, refers to the future – that it contributes to the action of the enemy. Shooting from a school may, in this case, constitute an indication. It is then necessary to determine, on the one hand, the level of destruction appropriate in the present circumstances (depending on the context) and, on the other hand, and above all, the expected military advantage of the attack. The attack on a military objective by use poses many questions, first and foremost, as to how the LAWSs can bring together these different conditions, particularly military advantage, when they require judgment. This is the decisive factor in attacking civilian object (Chengeta, 2016). Also, in the event that LAWSs are unable to produce such judgments (contribution to enemy action, military advantage), they cannot alone decide to attack military objectives by use. These will have to be designated by human beings, which greatly reduces the interest of the LAWS. Apart from the problems of respecting the principle of distinction, the introduction of these new means of combat also raises questions with regard to the concept of proportionality.

The Concept of Proportionality between Tension and Reinforcement

The new means and methods of warfare pose a challenge to the analysis of the proportionality concept (Boothby, 2013; Boylan, 2017). The concept of proportionality concerns two ideas. The first is the requirement to balance the harm caused to civil-

ians and the purpose of the attack (the principle of proportionality)[3]. The second dimension of proportionality is that, when there are several means to achieve a goal, the choice should be made in favour of the least harmful for civilians (the principle of precaution in attack).

The principle of precaution in attack as set out in article 57 of AP I requires measures to be taken in advance to avoid or at least minimize injury to civilians or damage to civilian objects. Compliance with this principle is not always respected, for example, in extrajudicial killing carried out by drones. Indeed, the timing and location of the attack are not always calculated to do the least harm to civilians.

The legality of LAWSs will also depend on the possibility of integrating into their programming the respect of the precautionary principle. This implies that the LAWS programming includes the obligation to choose between several objectives to minimize the risks and the obligation to cancel an attack in case of doubt. This raises the question of the non-neutrality of programming. This will be based on interpretations of the IHL of the possessor state, which can be questionable. Thus, the programming of Article 50 (1) of API by a French LAWS may be different from that of a LAWS of another state because France has issued an interpretative declaration on this rule. France and the United Kingdom consider that this rule 'cannot be interpreted as requiring the military command to take a decision which, depending on the circumstances and the information at its disposal, may not be compatible with its duty to ensure the safety of the troops under his responsibility or to preserve his military position in accordance with the other provisions of the Protocol'. On reading this statement, it seems that the 'preservation of the military situation' prevails over the protection of civilians. This demonstrates that LAWSs do not automatically lead to new problems and that, as with rules of engagement, the reactions of LAWSs may depend on the interpretation of each state integrated into the system.

The information available to the system and when it is acquired (during programming or during the attack) will also be important. Depending on the moment chosen, the information will not be the same and therefore the qualification of the attack may vary. Until now, the analysis of proportionality and the precautionary principle applied at the time the attack was decided. Consequently, an unexpected change in circumstances could not ipso facto be deemed sufficient to declare the attack illegal if, under the same circumstances and with the same information, a reasonable commander had made an identical decision. LAWSs could lead to an evolution of this interpretation since their sensors will enable them to acquire real-time information about the target. This capacity is reflected in the interpretation of the precautionary

[3] Article 51 (5) AP I.

principle since the moment when precautions can be taken is receded within a few seconds before the intended attack.

Then, paradoxically, the LAWSs could result in strengthening the precautionary principle. Indeed, the increase in information available could lead to a strengthening of the obligation to do everything possible to protect civilians. This conclusion is necessary in the light of what already applies to 'drones'. The use of these systems leads to a certain reinforcement of this obligation of behavior. This reinforcement is based on several reasons: real-time information, system autonomy and lack of life on the attacker's side. Each of these reasons reinforces the precautionary principle because it implies the possibility of waiting before triggering the attack (Herbach, 2012).

This principle is of great importance in the context of cyber war because civilian and military networks are intertwined. It is also important since there is no visibility of the target. The precautionary principle requires the target to be identified with a high degree of certainty. The attacker must be perfectly familiar with the network to be attacked. The attacker must also directly attack the target. This requires both computer skills and precise cyber weapons. Finally, the attacker must use methods and means of combat which have a high degree of probability of hitting the target whilst minimizing the risk to civilians. The use of cyber-attacks forces the military leader to carefully choose the type of attack.

The second dimension of proportionality requires the attacker to refrain from launching any attack which may be expected to cause incidental loss of life among civilians, injury to civilians, damage to civilian property, or a combination thereof, or damage which would be excessive in relation to the concrete and direct military advantage anticipated.

The application of this principle to cyber-attacks is quite complicated. It raises the question of what damage is to be taken into account for the analysis of proportionality. Cyberattacks produce different types of effects (Roscini, 2014, p. 52): immediate effects: destruction, corruption, data corruption, system damage, as happened in the Estonian and Georgian conflicts); destruction/neutralization of the machine or infrastructure like Stuxnet. Injury to civilians can result due to either, also like in Estonia or Georgia. If there is a poor assessment of the potential effects of the attack, a cyber-attack could be described as being indiscriminate (an attack in which attacker does not take into account potential civilian casualties) and would constitute a war crime. This situation could arise if the attack were aimed at all computers without trying to differentiate (e.g. a Botnets attack). The same is true if the cyber-attack is carried out with a cyber 'weapon' (virus etc.) (Mele, 2014) which cannot differentiate between military and civilian infrastructure. The principles of precaution in attack and proportionality impose an obligation to control the spread of a virus, so that the

cyber-attack affects only military infrastructure, or civilian objects in a proportionate manner. Stuxnet is a good example, because it was designed with the sole aim of attacking the Siemens system of Iranian centrifuges.

The principle of proportionality is of great importance in this discussion because it requires consideration of both direct and indirect effects (Rules 51 of *Tallinn manual*, (Schmitt, 2013)). The principle of proportionality requires not only a determination of the expected damage. Such damage must not be excessive in relation to the military advantage anticipated[45]. This requirement will pose problems for autonomous weapons systems. Are these systems able to determine if the damage is excessive or not? The problem is that the notion of 'military advantage' is contextual. The whole difficulty, therefore, lies in the interpretation of the term 'excessive'. This term does not refer to a quantitative assessment but involves a judgment. While civilian damage can be assessed fairly easily, the assessment of military advantage by LAWS is more problematic. For LAWS to be able to respect IHL, it would have to be able to measure the balance between military advantage and damage in order to determine whether, in this case, they would be excessive; In other words, the system should be able to forbid or stop a lawful attack, on the first analysis, because its result would be excessive. The fear is, of course, the continuation of this attack causing excessive damage compared to the concrete and direct military advantage expected in violation of articles 50 (1) and 52 (3) of API.

These new means of combat pose many difficulties which could lead to the adoption of new legal rules.

Towards the Creation of Specific Governances?

The difficulties related to the respect of the IHL by these new means of combat lead some scientists, lawyers and NGOs to ask for the adoption of new rules framing them (cyber weapons) or even banning them (LAWS). In other words, a specific governance for each of these new means of combat should be created because of their particular characteristics.

To this end, informal discussions on LAWS are a good example. Many NGOs have united, under the aegis of Human Rights Watch, in a militant group for a ban on 'robot killers'[6]. These NGOs require the conclusion of a Sixth Protocol to Convention

[4] Article 57 2) a) iii) AP I.

[5] Article 51 (5) b) AP I.

[6] Campaign to Stop Killer Robots, Article 36, Association for Aid and Relief, Japan, Facing Finance, Human Rights Watch, ICBL-CMC Austria, International Committee on Robot Arms

on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW), which would ban LAWSs. Under the pressure of this collective, the states, led by France, initiated informal discussions of experts, to better define the ethical, legal and operational debates surrounding the deployment of LAWS. These discussions have been ongoing since 2014. The particularity of these discussions is to bring together experts and representatives of states, as well as experts and representatives of NGOs. This configuration is very interesting because it allows the states, which are far from sharing the same opinions on the subject, and the NGOs, who are very critical, to express their position very upstream. This allows all stakeholders to meet and discuss in a formal and informal way. The three expert meetings of 2014, 2015 and 2016 thus highlighted, above all, the divergences existing between states and between states and NGOs.

First, there are divergences in the normative choice. Three positions emerged. A first group militates for a complete ban, for the adoption of a prohibitive treaty. A second group of experts advocates a regime of normative control of armaments, limiting only the specific characteristics of autonomous weapon systems or limiting the context in which they may be used. Finally, a third group advocates an adaptive normative approach consisting of a 'progressive evolution of codes of conduct based on traditional legal and ethical principles governing arms and war' (Dunn Cavelty, Fischer, & Balzacq, 2016). Differences, then, around four key points: the questions of definition including autonomy, responsibility, examination of weapons and human control.

These discussions, which for the time being are informal, should become formal from 2017 onwards. A non-binding recommendation, adopted at the April 2016 meeting, invites states Parties to the Convention to formally establish a group of governmental experts (GGE) at the next Review Conference, which December 2016. If the Review Conference agrees to follow this recommendation, GGE would meet in 2017 and 2018 to 'explore and agree on possible recommendations on options for emerging technologies in LAWS'[7]. These options range from new discussions to the negotiation of an instrument to regulate or ban autonomous weapons systems.

Control (ICRAC), Mines Action Canada, Nobel Women's Initiative, PAX, Pugwash Conferences on Science and World Affairs, Women's International League for Peace and Freedom; Friends World Committee for Consultation (Quakers), Geneva International Centre for Humanitarian Demining (GICHD), International Institute of Humanitarian Law, International Studies Association (ISA), PAX, Peace Research Institute Frankfurt (PRIF), Wildfire and World Council of Churches.

[7] Recommendations to the 2016 Review Conference Submitted by the Chairperson of the Informal Meeting of Experts.

However, a negotiating mandate on the subject seems unlikely as the majority of states do not see the need for negotiations on a sixth CCW protocol at this time. A continuation of the interviews with the participation of exhibitors of the civil society seems realistic.

The governance of cyber-weapons could follow a similar path. However, as with LAWS, the creation of hard law rules should not be immediate, as states are not prepared to enter into a treaty, in particular because they wish to have recourse to these new weapons. For this reason, the primary purpose of cyber-weapon regulation could be non-proliferation, i.e. the prevention of non-dissemination of cyber-arms. This limitation of the multiplication of the number of holders of this type of weapon can be directed either to non-holder states or to non-state actors. The second path seems to be the one most likely to prosper. The former would be difficult to accept by all states, while the latter could be the subject of a broad consensus.

The creation of these governances could follow several scenarios. The first, the most relevant for international security, would be the adoption of a treaty setting out specific obligations (hard law). Three possible assumptions can be envisaged: the negotiation of a treaty regulating globally cyber-arms and LAWS such as the Chemical Weapons Convention, the negotiation of treaties relating to certain cyber-weapons or certain types of LAWS (the treaty could thus limit their use to targets, targeting criteria, etc.), or the negotiation of a framework treaty to be supplemented by subsequent protocols.

However, the adoption of armaments rules is only feasible if certain conditions are met. First, the technology must be of concern. Under this condition, certainly, the LAWS framework will be faster because of the concerns they arouse, while the use of the cyber weapons whose use causes a lesser degree of concern have not yet given rise to a demand for regulation (Meyer, 2011).

Second, regulation requires the existence of an environment conducive to the conclusion of arms control agreements (Viotti, 2012). However, this context is not fully met. While there is an obvious interest in combating proliferation, the first and most powerful states wish to develop their arsenal in this area. As the history of arms control shows, the treaties governing new technologies are often concluded only after these technologies have been used for some time and have revealed gaps or shortcomings in the existing law or risks to National or international security (Sitaraman, 2009).

Therefore, at this stage, the adoption of legally binding international treaty-type rules that might involve regulatory or prohibition measures seems unlikely. As a first step, the standards should therefore fall under the soft law category. States could thus opt for the creation of codes of good conduct. This time neither the agreement nor

the content is legally binding. This does not mean that such an agreement would not be respected, it would be binding, but politically. These codes of conduct could seek to increase transparency and confidence in cyber-weapon intentions.

Conclusion

Applying IHL to these new technologies and means of combat can be tricky. However the difficulty in doing so has been exaggerated. While the weapons and tactics may change, the principals are far from new, they are inherent in IHL. Indeed, states wish to be able to retain certain latitude in the application of IHL. Challenges usually arise when such developments raise wider questions as to what are the acceptable ethical limits in the application of technology to military purposes (Stewart, 2009). Today, this leeway is being challenged by non-state actors (IOs, NGOs) which are lobbying for a more humane vision, ethical approach to dealing with and conducting armed conflicts.

There is an interrelationship between the challenges to the law and the law. If challenges raise the question of the relevance, application, or interpretation of the law, the law questions in turn the use of technologies and the means of combat in the contemporary conflict. IHL can govern contemporary conflicts because its principles are adaptable to new challenges. In fact, the real danger for the law of armed conflict is the impact of ideological interpretations which distort the law. IHL is therefore not obsolete. It is a relevant framework provided that it is implemented. The challenges discussed in this paper reveal that the issue is not so much about the relevance of the legal framework as it is about its application, its interpretation, and by extending the existence of a genuine international community.

So the question raised by evolutions in weapons technology dealt with in this article is concerning the need to create an arms control regime; in other words, a governance of cyber-weapons, a governance of military robotics. Once again, the main problem is not legal, but political. Hence, the main conclusion, which is not revolutionary in itself, is that the creation of a framework for these new means of combat depends on the will and interests of the states.

References:

Allan, C. (2013). "Direct participation hostilities from cyberspace". *Virginia Journal of International Law*, *54* (1), 173–193.

Bhuta, N., Beck, S., Geiß, R., Liu, H.Y., & Kreβ, C. (2016). *Autonomous Weapons Systems*. Cambridge: Cambridge University Press.

Boothby, W. (2013). "How Far Will the Law Allow Unmanned Combat Systems Comply with International Humanitarian Law". In D. Saxon (Ed.), *International Humanitarian Law and the Changing Technology of War* (pp. 45–64). Leiden: Martinus Nijhoff Publishers.

Boothby, W.H. (2014). *Conflict law: the influence of new weapons technology, human rights and emerging actors*. The Hague: Springer.

Bousquet, A.J. (2011). *The Scientific Way of Warfare*. Columbia University Press.

Boylan, E. (2017). "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners". *Vanderbilt Journal of Transnational Law*, *50*, 217–244.

Chengeta, T. (2016). "Measuring Autonomous Weapon Systems Against International Humanitarian Law Rules". *Journal of Law & Cyber Warfare*, *5* (1), 63–137.

Crawford, E. (2016). "From Inter-state and Symmetric to Intra-state and Asymmetric: Changing Methods of Warfare and theLaw of Armed Conflict in the 100 Years Since World War One". In T.D. Gill (Ed.), *Yearbook of International Humanitarian Law 2014* (pp. 95–118). The Hague: T.M.C. Asser Press.

Dunn Cavelty, M., Fischer, S.-C., & Balzacq, T. (2016). "«Killer Robots» and Preventive Arms Control". In V. Mauer & M. Dunn Cavelty (Eds.), *The Routledge Handbook of Security Studies* (pp. 457–468). London: Routledge.

Geiß, R. (2013). "Cyber Warfare: Implications for Non-international Armed Conflicts". *International Law Studies*, *89*, 627–645.

Geiß, R., & Lahmann, H. (2012). "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space". *Israel Law Review*, *45* (3), 381–399.

Gill, T.D. (2016). *Yearbook of International Humanitarian Law 2014*. The Hague: T.M.C. Asser Press.

Glennon, M.J. (2010). *The Fog of Law*. Stanford University Press.

Herbach, J.D. (2012). "Into the Caves of Steel: Precaution, Cognition and Robotic Weapon Systems Under the International Law of Armed Conflict". *Amsterdam Law Forum*, *4:3*, 3–20.

ICRC. (2016). *Commentary on the First Geneva Convention*. Cambridge: Cambridge University Press.

International Law Association (2010). *Final Report on the Meaning of Armed Conflict in International Law*. The Hague Conference.

Kaldor, M. (2012). *New and old wars: Organised violence in a global era*. Cambridge: Cambridge: Polity Press.

Lemieux, F. (2015). *Current and Emerging Trends in Cyber Operations*. London: Springer.

Lin, H. (2012). "Cyber conflict and international humanitarian law". *International Review of the Red Cross*, *94*, 515–531.

Mele, S. (2014). "Legal Considerations on Cyber-Weapons and Their Definition". *Journal of Law & Cyber Warfare*, *3* (1), 52–69.

Melzer, N. (2009). *Interpretive Guidance on the Notion of Direct Participation in Hostilities*. Geneva: ICRC.

Meyer, P. (2011). "Cyber-security through arms control". *The RUSI Journal*, *156* (2), 22–27.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.

Schmitt, M.N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.

Sitaraman, S. (2009). *State Participation in International Treaty Regimes*. Burlington: Ashgate Publishing.

Stewart, D.M. (2009). "New Technology and the Law of Armed Conflict". *International Law Studies*, *87*, 271–298.

Van Creveld, M.L. (1991). *Technology and war: from 2000 B.C. to the present*. New York: The free Press.

Viotti, P.R. (2012). "A Template for Understanding Arms Control". In R.E. Williams Jr & P.R. Viotti (Eds.), *Arms Control. History, Theory, and Policy* (pp. 7–14). Santa Barbara: Praeger.

Wilmshurst, E. (2012). *International Law and the Classification of Conflicts*. Oxford: Oxford University Press.

Author

Dr Eric Pomès

Catholic University of the Vendée (ICES). Contact details: 17 Boulevard des Belges, 85017 La Roche-sur-Yon, France; e-mail: epomes@ices.fr.