ICRC

International Humanitarian Law and New Weapon Technologies

Statement | GENEVA, 08 SEPTEMBER 2011.

34th Round Table on Current Issues of International Humanitarian Law, San Remo, 8-10 September 2011. Keynote address by Dr. Jakob Kellenberger, President, ICRC

Mr. President of the Institute,
Your Excellencies,
Ladies and Gentlemen,

New technologies and new weapons have revolutionised warfare since time immemorial. We need only think about the invention of the chariot, of canon powder, of the airplane or of the nuclear bomb to remember how new technologies have changed the landscape of warfare.

Since the St. Petersburg Declaration of 1868, which banned the use of projectiles of less than 400 grammes, the international community has attempted to regulate new technologies in warfare. And modern international humanitarian law has in many ways developed in response to new challenges raised by novel

weaponry. At the same time, while banning a very specific weapon, the St. Petersburg Declaration already set out some general principles which would later inform the entire approach of international humanitarian law towards new means and methods of warfare. It states that the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy, and that this object would be exceeded by the employment of arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable.

In this spirit, the regulation of new means and methods of warfare has developed along two tracks for the last 150 years: The first consists of **general principles and rules that apply to all means and methods of warfare**, as a result of the recognition that the imperative of humanity imposes limits to their choice and use. The second consists of **international agreements which ban or limit the use of specific weapons** – such as chemical and biological weapons, incendiary weapons, anti-personnel mines, or cluster munitions.

The general principles and rules protect combatants against weapons of a nature to cause superfluous injury or unnecessary suffering but have also developed to protect civilians from the effects of hostilities. Thus, for example means and methods of warfare that are indiscriminate are prohibited.

Informed by these fundamental general prohibitions, international humanitarian law was designed to be flexible enough to adapt to technological developments, including those that could never have been anticipated at the time. There can be no doubt that international humanitarian law applies to new weaponry and to all new technology used in warfare. This is explicitly recognised in article 36 of Additional Protocol I, according to which, in the study, development or adoption of a new weapon or method of warfare, states parties are under an obligation to determine

whether their employment would, in some or all circumstances, be prohibited by international law applicable to them.

Nonetheless, applying pre-existing legal rules to a new technology raises the question of whether the rules are sufficiently clear in light of the technology's specific – and perhaps unprecedented characteristics, as well as with regard to the foreseeable humanitarian impact it may have. In certain circumstances, States will choose or have chosen to adopt more specific regulations.

Today, we live in the age of information technology and we are seeing this technology being used on the battlefield. This is not entirely new but the multiplication of new weapons or methods of warfare that rely on such technology seems exponential. The same advances in information technology that enable us to have live video chat on our mobile phones also make it possible to build smaller, less expensive, and more versatile drones. The same technology used for remote controls of home air conditioning units also makes it possible to turn off the lights in a city on the other side of the globe. This year's Round Table will allow us to take a closer look and to discuss a number of technologies that have only recently entered the battlefield or could potentially enter it. These are, in particular cyber technology, remote controlled weapon systems, and robotic weapon systems.

Let me first turn to "**cyber warfare**".

The interest in legal issues raised by "cyber warfare" is currently particularly high. By cyber warfare I mean means and methods of warfare that rely on information technology and are used in the context of an armed conflict. The military potential of cyber space is only starting to be fully explored. From certain cyber operations that have occurred, we know that one party to a conflict can potentially "attack" another party's computer systems, for instance by infiltrating or manipulating it. Thus, the cyber

infrastructure on which the enemy's military relies can be damaged, disrupted or destroyed. However, civilian infrastructure might also be hit – either because it is being directly targeted or because it is incidentally damaged or destroyed when military infrastructure is targeted.

So far, we do not know precisely what the humanitarian consequences of cyber warfare could be. It appears that technically, cyber attacks against airport control and other transportation systems, dams or nuclear power plants are possible. Such attacks would most likely have large scale humanitarian consequences. They could result in significant civilian casualties and damages. Of course, for the time being it is difficult to assess how likely cyber attacks of such gravity really are, but we cannot afford to wait until it is too late to prevent worst case scenarios.

From a humanitarian perspective, the main challenge about cyber operations in warfare is that cyberspace is characterized by interconnectivity and thus by the difficulty to limit the effects of such operations to military computer systems. While some military computer infrastructure is certainly secured and separated from civilian infrastructure, a lot of military infrastructure relies on civilian computers or computer networks. Under such conditions, how can the attacker foresee the repercussions of his attack on civilian computer systems? Very possibly, the computer system or connection that the military relies on is the same as the one on which the hospital nearby or the water network relies.

Another difficulty in applying the rules of international humanitarian law to cyberspace stems from the digitalisation on which cyberspace is built. Digitalisation ensures anonymity and thus complicates the attribution of conduct.

Thus, in most cases, it appears that it is difficult if not impossible to identify the author of an attack. Since IHL relies on the at-

tribution of responsibility to individuals and parties to conflicts, major difficulties arise. In particular, if the perpetrator of a given operation and thus the link of the operation to an armed conflict cannot be identified, it is extremely difficult to determine whether IHL is even applicable to the operation.

The second technological development that we will be discussing at this Round Table are **remote-controlled weapon systems**.

Remote controlled weapon systems are a further step in a long-standing strategic continuum to move soldiers farther and farther away from their adversaries and the actual combat zone.

Drones – or "unmanned aerial vehicles" are the most conspicuous example of such new technologies, armed or unarmed. Their number has increased exponentially over the last few years. Similarly, so called unmanned ground vehicles are increasingly deployed on the battlefield. They range from robots to detect and destroy roadside bombs to those that inspect vehicles at approaching checkpoints.

One of the main arguments to invest in such new technologies is that they save lives of soldiers. Another argument is that drones, in particular, have also enhanced real time aerial surveillance possibilities, thereby allowing belligerents to carry out their attacks more precisely against military objectives and thus reduce civilian casualties and damage to civilian objects – in other words to exercise greater precaution in attack.

There could be some concern, however, on how and by whom these systems are operated. Firstly, they are sometimes operated by civilians, including employees of private companies, which raises a question about the status and protection of these operators and questions about whether their training and accountability is sufficient in light of the life and death decisions that they make. Secondly, studies have shown that disconnecting a person,

especially by means of distance (be it physical or emotional) from a potential adversary makes targeting easier and abuses more likely. The military historian John Keegan has called this the "impersonalization of battle".

Lastly, let me say a few words about **robotic weapon systems**.

Automated weapon systems – robots in common parlance – go a step further than remote controlled systems.

They are not remotely controlled but function in a self-contained and independent manner once deployed.

Examples of such systems include automated sentry guns, sensor fused munitions and certain anti-vehicle landmines. Although deployed by humans, such systems will independently verify or detect a particular type of target object and then fire or detonate. An automated sentry gun, for instance, may fire, or not, following voice verification of a potential intruder based on a password.

The central challenge with automated systems is to ensure that they are indeed capable of the level of discrimination required by IHL. The capacity to discriminate, as required by IHL, will depend entirely on the quality and variety of sensors and programming employed within the system. Up to now, it is unclear how such systems would differentiate a civilian from a combatant or a wounded or incapacitated combatant from an able combatant.

Also, it is not clear how these weapons could assess the incidental loss of civilian lives, injury to civilians or damage to civilian objects, and comply with the principle of proportionality.

An even further step would consist in the deployment of autonomous weapon systems, that is weapon systems that can learn or adapt their functioning in response to changing circumstances. A truly autonomous system would have artificial intelligence

that would have to be capable of implementing IHL. While there is considerable interest and funding for research in this area, such systems have not yet been weaponised. Their development represents a monumental programming challenge that may well prove impossible. The deployment of such systems would reflect a paradigm shift and a major qualitative change in the conduct of hostilities. It would also raise a range of fundamental legal, ethical and societal issues which need to be considered before such systems are developed or deployed. A robot could be programmed to behave more ethically and far more cautiously on the battlefield than a human being. But what if it is technically impossible to reliably program an autonomous weapon system so as to ensure that it functions in accordance with IHL under battlefield conditions?

When we discuss these new technologies, let us also look at their possible advantages in contributing to greater protection. Respect for the principles of distinction and proportionality means that certain precautions in attack, provided for in article 57 of Additional Protocol I, must be taken. This includes the obligation of an attacker to take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental civilian casualties and damages. In certain cases cyber operations or the deployment of remote controlled weapons or robots might cause fewer incidental civilian casualties and less incidental civilian damage compared to the use of conventional weapons. Greater precautions might also be feasible in practice, simply because these weapons are deployed from a safe distance, often with time to choose one's target carefully and to choose the moment of attack in order to minimise civilian casualties and damage. It may be argued that in such circumstances this rule would require that a commander consider whether he or she can achieve the same military advantage by using such means and methods of warfare, if practicable.

Ladies and Gentlemen,

The world of new technologies is neither a virtual world nor is it science fiction. In the real world of armed conflict, they can cause death and damage. As such, bearing in mind the potential humanitarian consequences, it is important for the ICRC to promote the discussion of these issues, to raise attention to the necessity to assess the humanitarian impact of developing technologies, and to ensure that they are not prematurely employed under conditions where respect for the law cannot be guaranteed. The imperative that motivated the St. Petersburg Declaration remains as true today as it was then.

I thank the Institute of International Humanitarian Law for hosting this Round Table and thank all of you for your interest in engaging with us in reflection and debate. I wish you fruitful and successful discussions.