Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

REPORTS AND DOCUMENTS

International Humanitarian Law and New Weapon Technologies, 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011

Keynote address by Dr Jakob Kellenberger, ICRC President, and Conclusions by Dr Philip Spoerri, ICRC Director for International Law and Cooperation

: : : : : : :

Keynote address by Dr Jakob Kellenberger, President, International Committee of the Red Cross*

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.

* Also available at: http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm

doi:10.1017/S1816383112000793

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 attribution 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.

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.

Conclusions by Dr Philip Spoerri, Director for International Law and Cooperation, International Committee of the Red Cross*

The panels of this conference have touched upon a myriad of new technologies, ranging from energy weapons, to drones, robots, satellite technology and space weapons and cyber technology. Some of these technologies are already deployed on today's battlefields, others are still in the realm of science fiction.

The discussions revealed a number of overarching themes, providing food for thought and for further research and thinking. I cannot attempt to summarize all of them, but I would like to highlight five aspects that appeared to be recurring.

Firstly, our discussions revealed a measure of **uncertainty about the facts**. It is not always clear what is technically feasible in today's theatres of war, and less clear what will be feasible in the future and when. It is also not always clear what the humanitarian impact is – of weapons that are already deployed, like drones; that are ready to be deployed, like cyber attacks; or that might be deployed in the future, like autonomous robots. To what extent does this uncertainty hamper our ability to ensure that all new technologies in warfare comply with international humanitarian law? My impression is that while the uncertainty about the specificities and impact of some of these technologies does pose a challenge to applying the law to them, this challenge should not be overstated.

In cyber warfare, for instance, anonymity and interconnectedness of computer networks around the world do indeed seem to pose very serious questions about the way international humanitarian law will play out in the cyber realm. More exchange will need to take place between scientists and lawyers to get clarity on these issues. On the other hand, there seems to be little doubt that cyber attacks are feasible now and can potentially have devastating effects on civilians and civilian infrastructure, for instance by causing the disruption of air control systems, or electricity or water supply systems. Most of us have little or no understanding of how information technology works, and yet there are a number of things we already know and can already say about which effects would be lawful or not should they occur. Most of us do not know how to fly airplanes, but we know about the effects of aerial bombing. In this sense, we should concentrate on the effects of technology we see today in warfare ('in the real world'), and we will probably be able to go a long way in being able to make reasoned statements about the applicability of international humanitarian law and the lawfulness of specific means and methods of warfare in cyber space.

Secondly, the fact that **new technologies remove soldiers further and further away from the battlefield** was a matter of recurring discussion. Many discussants pointed out that remoteness of the soldier to the enemy is nothing fundamentally new. Yet, it is also apparent that a common feature of the new technologies under discussion is that they appear to carry distance one step further – be it by remote-controlled weapons, cyber weapons or robots.

* Also available at: http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm

doi:10.1017/S181638311200080X

More thinking is required about the consequences of these remote means and methods of warfare. Firstly, what is the consequence of their use for the definition, the extent of the battlefield? Some have argued that if drones can be flown or cyber attacks launched from anywhere in the world, then anywhere in the world becomes a battlefield. This would in effect be an endorsement of the concept of a 'global battlefield', with the consequence that the use of force rules allowing for incidental civilian loss and damage under the IHL principle of proportionality extend far beyond the scope of what has until now been accepted. This is a notion that the ICRC does not follow.

Long distance means and methods of warfare also pose some questions as to the relationship between, *on the one hand, the use of new technologies to keep soldiers out of harm's way by limiting their exposure to direct combat, and on the other hand their humanitarian impact for the civilian population*. It is probably impossible to say that the remoteness of soldiers from the battlefield will by itself create greater risks for civilians. But given the aversion of many societies and governments to risk the lives of their soldiers, there is a danger that the tendency towards so-called zero casualty wars could lead to choices of weapons that would be dictated by this concern, even if it went to the detriment of the rules of international humanitarian law that protect civilians against the effects of hostilities. Just like high altitude bombing might be safer for soldiers but also in certain circumstances indiscriminate and unlawful, so new technologies, however protective for the troops, will always have to be tested for their compatibility with humanitarian law and in particular their possible indiscriminate or disproportionate effects. This, however, requires that we get a better understanding about the effects of such technologies, in particular their precision and their incidental effects – not only in abstract technological terms but in the way they are concretely being used.

This leads me to a third point, which is a certain **lack of transparency about the effects of certain weapons for the civilian population** – not their potential effect in the future, but the effect of those technologies that are already being used. For instance, there is controversy about the effects of drones: no one appears to know with any measure of certainty the loss of civilian lives, injury to civilians and damage to civilian infrastructure that has been caused by drone attacks. The lack of objective knowledge constitutes a great impediment for the assessment of the lawfulness of weapons or their use in particular circumstances. Transparency in recording the humanitarian consequences of new technologies would certainly be of benefit in this respect – because it would already take into account not only the abstract technical specificities but integrate the actual way in which they are used.

As we heard, however, **new technologies can actually also be tools for more transparency, namely to support the witnessing, recording and investigation of violations**. We heard a very interesting presentation about this in relation to satellite images used by UNITAR to investigate violations during armed conflict. Other technologies come to mind: for instance DNA technology which can sometimes complement traditional forensic science methods, or simple devices such as mobile phone cameras that have been used to record violations. The limits of

using images to illustrate or prove violations in armed conflict, in particular war crimes, is not something new and it is well known that images rarely speak for themselves. But new technologies – together with traditional means, in particular witness accounts – can contribute to uncovering certain violations and this must surely be welcomed.

A fourth recurring theme was that of **responsibility and accountability for the deployment of new technologies**. Whether new technologies will reduce our capacity to allocate responsibility and accountability for violations remains to be seen. As a starting point, it is worth recalling that international humanitarian law parties to conflicts (states and organised armed groups) and international criminal law binds individuals. Just as a number of speakers pointed out, I am not convinced that we have reached the end of accountability with autonomous weapons. Even if artificial intelligence were to be achieved and autonomous systems deployed in armed conflicts, would it not always be the case that any robot is at some point switched on by a human being? If that is the case, then that individual – and the party to the conflict – is responsible for the decision, however remote in time or space the weapon might have been deployed from the moment of the attack. It is a topic that reminds me of Goethe's poem *Der Zauberlehrling* ('the sorcerer apprentice'), who unleashed a broom with destructive artificial intelligence and UAV capacity. Both the apprentice and the magician himself certainly bore their share of responsibility and the magician ultimately had to put his house in order. In cyber space on the other hand, allocation of responsibility does appear to present a legal challenge if anonymity is the rule rather than the exception.

Lastly, the most recurrent overarching theme was maybe that **technology, in itself, is neither good nor bad. It can be a source of good and progress or result in terrible consequences at worst**. This is true most of the time. Transposed to technologies that are weaponised, this means that most weapons are not unlawful as such; whether their use in conflict is lawful or not depends on the circumstances and the way in which they are used.

This being said, some weapons are never lawful and have been banned – blinding laser weapons or landmines, for instance. The same will be true for new technologies: the lawfulness of new means and methods of warfare will usually depend on their use, but it is not excluded that some weapons will be found to be inherently indiscriminate or to cause superfluous injury or suffering, in which case they will have to be banned. This is why the principle reflected in Article 36 of Additional Protocol I that States should verify, when developing new means and methods of warfare, whether their use will be compatible with international humanitarian law is so critical.

If we can draw a lesson from past experience – for instance the deployment of the nuclear bomb – it is that we have trouble anticipating the problems and disasters that we might face in the future. Some say that robots or other new technologies might mean the end of warfare. If robots fight robots in outer space without any impact on human beings other than possible economic loss this would look like the world of knights fighting duels on a meadow outside the city gates, a fairy outcome short of war. But since this is a very unlikely scenario, we have to

focus on the more likely scenario that technologies in armed conflicts will be used to cause harm to the enemy, and that this harm will not be limited to purely military targets but will affect civilians and civilian infrastructure.

So, indeed, let us not be overly afraid about things that might not come – this was the credo of many speakers here in San Remo. But let us nonetheless be vigilant and not miss the opportunity to recall, every time it is needed, that the fundamental rules of international humanitarian law are not simply a flexible moral code. They are binding rules, and so far they are the only legal tool we have to reduce or limit, at least to a small extent, the human cost of war. A multi-disciplinary meeting such as this roundtable is an excellent means to advance towards this goal.