STATEMENT

AALCO Working Group on International law in Cyber Space

Thank you Chair, for giving the International Committee of the Red Cross (ICRC) this opportunity to address the important issue of the legal implications of cyber warfare.

His Excellency, Professor Kennedy Gastorn, Secretary-General of the Asian-African Legal Consultative Organisation (AALCO),

AALCO Deputy Secretaries-General,

Your Excellencies,

Distinguished Delegates,

Ladies and Gentlemen,

Let me first thank AALCO for the strong partnership we share since the signing of our Memorandum of Understanding in 2003 to work together for the promotion, dissemination and implementation of international humanitarian law (IHL). On behalf of the ICRC, I am honoured to open this session on the legal implications of cyber warfare.

Throughout human history and the history of warfare, warring parties have turned to new weapons and new technologies to gain an advantage over their adversaries. Today some States and other parties to armed conflicts look to cyber technology as an enabler with the same objective. The security, legal and humanitarian concerns raised by the use of new technologies in armed conflicts have sparked intense debates, and cyber warfare is no exception. The ICRC has outlined some of these challenges in its 2015 Report on IHL and the Challenges of Contemporary Armed Conflicts.[1]

Today I will be focusing my remarks on cyber warfare, but before going any further, I would like to take a moment to cover:

[1] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* Geneva, Switzerland, October 2015, available at: https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf, pp 38-44.

Who are we and why are we concerned?

The ICRC is a neutral independent humanitarian organisation directed by its international mandate to protect and assist victims of armed conflicts, and work for the faithful application of IHL.

The legality of any resort to force by States, whether through cyber or kinetic means, is governed first by another body of law, the law on the use of force or *jus ad bellum* as reflected in the UN Charter. It requires States to refrain from the threat or use of force while preserving the right of individual or collective self-defence in response to an armed attack and permits the UN Security Council to sanction the use of force to maintain international peace and security.

For its part, IHL, also known as *jus in bello,* applies *during* an armed conflict and governs *how* States or other parties to a conflict use force. The aim of IHL is to mitigate suffering, by protecting those who are not, or are no longer, participating in hostilities, and by restricting the means and methods of warfare that parties to armed conflicts may employ. It protects persons and objects affected by armed conflict irrespective of the lawfulness of the first resort to force and irrespective of the party to which they belong.

The ICRC's concern with any weapon is based on the humanitarian consequences of its use and its compatibility with IHL. As a frontline humanitarian organization, our presence on the ground in conflict situations causes us to witness the impact of all weapons, old and new, and drives our efforts to call on States to limit their use by clarifying or developing the law. As far back as WW I, the ICRC called on States to prohibit the use of poisonous and asphyxiating gases based on our first hand observation of their high human cost, contributing to the adoption of the Geneva Gas Protocol in 1925. We encouraged States to bring in bans for anti-personal mines and cluster munitions, we work to clear unexploded ordinance and help affected communities avoid the risks, or to recover and rehabilitate from their injuries or losses.

Fortunately, cyber warfare has not led to dramatic humanitarian consequences to date. While the military potential of cyberspace is not yet fully understood, it nevertheless appears that cyber-attacks against transportation systems, electricity networks, dams, and chemical or nuclear plants are technically possible. Such attacks could have wide-reaching consequences. There are also concerns that cyber operations could be used to cause civilian infrastructure or services to malfunction. The effects of such "bloodless" attacks could obviously be severe – for instance, if power or water supplies were to be interrupted or if a banking system were to be taken down. Therefore, there is an urgency to take practical steps with a view to clarifying the limits that IHL already imposes on the resort to cyber as a means of warfare. I am convinced your discussions today will help advance this process.

What is cyberwarfare?

There is no universally agreed definition of cyberwarfare or cyberattack under international law.

A large proportion of operations referred to as "cyberattacks" in fact constitute illicit information gathering, such as espionage or other cybercrimes, occur outside the context of an armed conflict and are not governed by IHL. While they raise cyber security concerns, they fall below the threshold of an armed conflict and will be discussed during the following session on Cybercrimes and International Law.

For the ICRC, cyber warfare refers to operations against a computer or a computer system through a data stream, when used as means and methods of warfare in the context of an armed conflict. This can occur in two situations: as part of an armed conflict otherwise waged through kinetic operations, or through cyber means in the absence of kinetic operations when

their use amounts to an armed conflict - although no State is known to have publicly qualified an actual hostile cyber operation as such.

How does IHL regulate cyber warfare?

While IHL treaties do not expressly prohibit or regulate cyber warfare, there are limitations under IHL when parties to a conflict resort to cyber operations during an armed conflict. Indeed, support for applying existing IHL norms to cyber warfare can be found in the judgement of the International Court of Justice (ICJ) and the text of IHL treaties:

- The ICJ in its Advisory Opinion on the Threat or Use of Nuclear Weapons states that the established principles and rules of IHL apply to "all forms of warfare and all kinds of weapons" including "those of the future."[2]
- This is also made clear in the obligation to undertake a legal review of new weapons, to determine if their use is prohibited by international law as stipulated under Art. 36 of the First 1977 Additional Protocol to the Geneva Conventions.[3] Such reviews are indeed essential to ensure that new weapons comply with existing law including IHL norms and this is precisely because such norms apply to new weapons. Actually, all States have an interest in assessing the legality of new weapons regardless of whether they are party to Additional Protocol I. Indeed, the faithful and responsible application of its international law obligations would require any State to ensure that the new weapons, means and methods of warfare it develops or acquires will not violate these obligations.

The ICRC holds the position that if cyber means are employed during armed conflicts they must comply with IHL like any other means and methods of warfare, new or old. Over time, many States and international organizations have also asserted that cyberwarfare must comply with IHL.

In keeping with these developments, the 2013 and 2015 reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security confirmed that "international law, and particularly the Charter of the UN is applicable"[4] and noted "the established principles of humanity, necessity, proportionality and distinction."[5]

To assert that IHL applies to cyber warfare is not an encouragement to militarize cyberspace and should not, in any way, be understood as legitimizing cyber warfare. Indeed, as I mentioned earlier, any resort to force by States, whether cyber or kinetic, always remains governed by the UN Charter and *jus ad bellum*.

What limits does IHL place on the means and methods of warfare in general and in cyberwarfare?

IHL is based on a balance between military necessity and considerations of humanity. It allows - or at least does not prohibit - the use of lethal force against lawful targets. At the same time

---

[2] ICJ Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, para. 86.
[3] Art. 36 AP I: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party".
[4] UN Group of Governmental Experts on Developments in the Field of IT in the context of International Security, 24 June 2013, A/68/98, para. 19.
[5] UN Group of Governmental Experts, 22 July 2015 A/70/174, para. 28(d).

the use of lethal force is regulated by the rules on the conduct of hostilities, and in particular, the principles of distinction, proportionality and precautions, which aim to protect civilians and civilian objects from the effects of hostilities.

The principle of distinction requires belligerents to distinguish at all times between civilians and civilian objects on the one hand and combatants and military objectives on the other and direct their military operations only against the later. IHL also prohibits indiscriminate and disproportionate attacks. Furthermore, belligerents must take all feasible precautions, notably in the choice of means and methods of warfare, to avoid or minimize incidental harm to civilians and civilian objects.

All weapons, means and methods of warfare must be used, and must be capable of being used, in accordance with the rules governing the conduct of hostilities and the limitations they impose. Thus the parties to an armed conflict do not have an unlimited choice of means and methods of warfare.

Why is it important that IHL applies to cyberwarfare?

Allow me to use a few examples to illustrate why it is important that IHL applies to cyber warfare.

There is increasing concern in many countries about safeguarding essential civilian infrastructure against cyber-attacks. Facilities providing potable water and electricity networks that serve the civilian population, as well as public health infrastructure are civilian objects. The application of IHL to cyber warfare means that attacks against such objects are prohibited.

Similarly, dams and nuclear plants also enjoy special protection under IHL. They cannot be the object of attack, to avoid the release of dangerous forces that can cause severe losses among the civilian population.

Furthermore, IHL requires belligerents to respect and protect hospitals. Therefore, a cyber-attack that affects the information system of a hospital and manipulates patient medical records would violate IHL.

What are the challenges cyberwarfare raises for the interpretation and application of IHL?

While IHL offers a legal framework that is crucial to protect civilians and civilian objects from the effects of cyber warfare, its application to and interpretation for these new technologies raises several challenges. Let me mention a few key challenges:

- The first challenge relates to the interconnectedness of cyberspace and the conduct of hostilities principles of distinction and proportionality.

  There is only one cyberspace with the same networks, routers, cables and satellites shared by civilian and military users. Moreover military systems are often dependent on and inseparable from civilian cyber infrastructure. It is to a large extent impossible to distinguish between purely civilian and purely military cyber infrastructure. This creates major challenges for the application of the principle of distinction.

  However, even if certain parts of the cyber infrastructure were to become legitimate military objectives, any attack still remains governed by the prohibition of indiscriminate attacks and the rules on proportionality and precautions in attack.

- Second, assessing the expected incidental civilian harm (sometimes referred to as “collateral damage”) of any planned operation is an obligation under IHL. However, the

interconnectedness of the networks make it is difficult, if not impossible, to foresee the extent of expected incidental harm which must be assessed to meet the prohibition of indiscriminate and disproportionate attacks.

- A third challenge is about the notion of "attack", which is fundamental to the application of the rules on the conduct of hostilities. Indeed, most of the rules mentioned earlier apply to "attacks", which are defined by the First 1977 Additional Protocol as "acts of violence against the adversary, whether in offence or in defence."[6]

  This raises the question of whether a cyber operation aimed at making a network such as an electrical grid dysfunctional constitutes an "attack" in the first place and thus triggers the prohibition on direct attacks against civilian objects and the prohibition of indiscriminate and disproportionate attacks?

  At the heart of this issue is the question - what amounts to an "act of violence" in cyber space? Is "physical damage" only relevant, as some have argued? Or does loss of functionality of an object also constitute "damage"?

  For the ICRC, if an object is disabled, it is immaterial whether this occurred through physical destruction or any other way, and as noted this is very important in practice for cyber operations. In our view, an overly restrictive understanding of the notion of attack is difficult to reconcile with the object and purpose of the rules on the conduct of hostilities, namely to ensure the protection of the civilian population and civilian objects against the effects of hostilities.

- The last challenge I will mention is the anonymity in cyberspace, which complicates the ability to attribute aggressive activities to perpetrators. If the perpetrator of a cyberattack cannot be identified it may be difficult to determine if IHL is even applicable to the operation.

Recommendations

The issues outlined are of relevance to all States, not just those that possess or are developing cyber capabilities. In this respect, AALCO member States, can weigh in to shape these important discussions to promote measures that protect civilians and civilians objects from the effects of cyber warfare.

With your permission Mr. Chair, I will end with a few points that this AALCO working group could consider in its discussions:

- First, to clarify how the protection that IHL already affords to civilians and civilian objects should be interpreted and applied with regard to cyber operations.
- Second, to underscore the importance for States that develop or acquire cyber-warfare capabilities – whether for offensive or defensive purposes – to assess their lawfulness under IHL, and to call upon States to take practical steps to implement this obligation.
- Third, to discuss and identify, as technologies evolve or their humanitarian impact is better understood, whether there is a need for new norms. If so, such norms should build upon and strengthen the protection that already exists under IHL. It would therefore be of high interest for the working group to monitor and document the technological developments in cyber warfare, with a view to better understand its potential humanitarian impact and the risks it entails.
- From a more practical perspective, IHL requires that parties to a conflict take all feasible measures to protect civilians and civilian objects under their control against the effects of hostilities. This obligation needs to be implemented in peace time already. Measures

[6] AP I Art. 49(1).

that could be considered could include segregated computer systems on which essential civilian infrastructure depends from the internet, backing up important civilian data and using antivirus measures among others. This working group could consider identifying the most efficient measures States could adopt in this regard.

Once again the ICRC is delighted to support this AALCO open-ended working group and we reaffirm our commitment to work closely with it through our Legal Advisory Services.

To stop technological development is as futile as the proverbial story of King Canute's attempt to command the waves. Technology will only continue to evolve - impacting weapons and thus the way war is waged. However, we need to act responsibly to control the development and use of new weapons and address their legal and humanitarian consequences, before we are compelled to act because of their human cost. Only through collective efforts can we ensure that the obligation to respect IHL remains aligned with developments in the technology of warfare.

Thank you.