ICRC

United Nations Group of Governmental Experts

Informal open-ended consultative meeting

Thursday 5 December 2019

Statement by the International Committee of the Red Cross

Mr. Chairman,

Distinguished delegates,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to address the informal open-ended consultative meeting of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security.

In recent years, cyber operations have shown that essential civilian infrastructure – hospitals, power grids, even nuclear plants – are at risk of disruption through digital means. Until now, cyber operations outside the context of armed conflicts have dominated headlines. However, a few States have publicly acknowledged using cyber operations during armed conflicts, and a growing number of States are developing military cyber capabilities.

The ICRC submitted a position paper on *International Humanitarian Law and Cyber Operations during Armed Conflicts* to the Group of Governmental Experts and to the Open-Ended Working Group to support the deliberation of States.[1] We are honoured to present today five key points from the position paper.

Firstly, cyber operations can cause human harm.

During armed conflicts, cyber operations have been used in support of or alongside kinetic operations. By means of cyber operations, a variety of "targets" in the real world can be disrupted, altered or damaged, including industries, infrastructure, telecommunications, transport, or governmental and financial systems.

The ICRC is concerned by the potential human cost arising from the increasing use of cyber operations during armed conflicts. We are particularly worried about the vulnerability of the health-care sector to cyber attacks.[2]

Secondly, IHL applies to cyber operations during armed conflict.

Mr. Chairman,

In our view, there is no doubt that existing IHL principles and rules apply to the use of new weapons, means and methods of warfare during armed conflicts, including those relying on information and telecommunications technology. The interpretation that IHL applies to new

[1] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, 2019.

[2] See further ICRC, *The Potential Human Cost of Cyber Operations*, 2019.

weapons and forms of warfare has been endorsed by the International Court of Justice,[3] and is reflected in existing IHL treaties.[4]

However, asserting that IHL applies to cyber operations during armed conflict does not encourage the militarization of cyberspace or legitimize cyber warfare, just as it does not legitimize any other form of warfare. Any use of force by States remains governed by the Charter of the United Nations, in particular the prohibition on the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains. What IHL affords is an additional layer of protection for civilian populations in the unfortunate event of an armed conflict as it places stringent constraints on the conduct of the parties to the conflict.

Thirdly, IHL provides essential rules protecting civilian populations.

Existing IHL treaties and customary law govern many issues during armed conflict. With respect to cyber operations, the relevant rules and principles range from the principles of distinction, proportionality, and precautions to more specific rules, such as the prohibition to render useless objects indispensable to the survival of the population[5] or the prohibition of terrorizing the civilian population.[6]

Regarding the high vulnerability of the health-care sector to digital disruption, the ICRC emphasizes that existing IHL rules strictly prohibit direct attacks against medical units and personnel, which include attacks conducted through cyber means.[7]

Fourthly, there is a need to clarify how key IHL notions apply in cyberspace.

To afford protection to the civilian population against the effects of cyber operations, IHL principles and rules need to be understood and interpreted in a way that takes into account the specific characteristics of cyberspace.

[3] ICJ, *Legality of the Threat or Use of Nuclear Weapons Case* (Advisory Opinion) [1996] ICJ Rep 226, para. 86 (noting that the established principles and rules of humanitarian law applicable in armed conflict apply 'to all forms of warfare and to all kinds of weapons', including 'those of the future').

[4] See Art. 36 of the 1977 First Additional Protocol to the four 1949 Geneva Conventions (hereafter 'AP I').

[5] Art. 54(2) AP I; Art. 14 of the 1977 Second Additional Protocol to the four 1949 Geneva Conventions (hereafter 'AP II'); Rule 54 ICRC Customary IHL Study.

[6] Art. 51(2) AP I; Art. 13(2) AP II; Rule 2 ICRC Customary IHL Study.

[7] See, for instance, Art. 19 of the 1949 First Geneva Convention; Arts 22 and 39 of the 1949 Second Geneva Convention; Art. 18 of the 1949 Fourth Geneva Convention; Art. 12 AP I; Art. 11(1) AP II; Rules 25, 28, 29, and 30 ICRC Customary IHL Study.

For instance, the notion of 'attack' under IHL requires clarification in the cyber context.[8] It is widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL.

At the ICRC, we have repeatedly emphasized our view that an operation designed to disable a computer or a computer network during an armed conflict also constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means.[9] Specifically, it is our view that a cyber operation designed to make a civilian network dysfunctional during an armed conflict would constitute a prohibited attack under IHL.

Finally, any development of law or norms must build on existing rules.

Mr. Chairman,

The use of cyber operations as means or methods of warfare in an armed conflict poses a real risk of harm to civilians.

In the ICRC's view, it is now critical for the international community to affirm the application of IHL to cyber operations during armed conflict and reach common understandings on how IHL applies.

We all have a shared responsibility to uphold the norms that safeguard our humanity even in the midst of armed conflict, in cyberspace just as in the physical world.

At the ICRC, we stand ready to lend our expertise to such discussions.

Thank you.

[8] For the purposes of IHL, Art. 49 AP I defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. The notion of attack under IHL is different from and should not be confused with the notion of 'armed attack' under Art. 51 of the UN Charter, which belongs to the realm of *jus ad bellum*. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

[9] See ICRC, *International Humanitarian Law and the challenges of contemporary armed conflicts*, 2011, p. 37; ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015, pp. 41-42.