ICRC

United Nations cyber consultations with all stakeholders

Segment "Creating a cyber space based on rules, laws and norms: How can stakeholders support governments"

Monday 2 December 2019

Scene-setting presentation

Mr. Chairman,

Distinguished delegates,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to address this consultative meeting.

Over the 156 years of its existence, the ICRC has seen armed conflicts change dramatically. However, what remained constant is our firm conviction that a clear framework of rules helps save lives and reduce suffering, a conviction rooted in our work with people affected by armed conflict throughout this time. This is the case whether the humans are endangered by revolvers and muskets – or by rootkits and malware.

In recent years, a range of cyber operations against essential civilian infrastructure – including hospitals, electrical grids, and even nuclear plants – have underscored the risk that digital means pose to the civilian population. At the ICRC, we have engaged in extensive discussions with experts from all over the world and conducted our own research to examine the potential human cost of cyber operations. Our findings, published earlier this year, show for instance that the health-care sector is particularly vulnerable to cyber attacks, due to the increased digitization and interconnectivity of medical devices.[1] We are also concerned about the increased frequency of cyber attacks against industrial control systems, such as those used to operate essential civilian services, including water and sanitation facilities.[2]

Mr. Chairman,

In the ICRC's view, any discussion on fostering a rules-based cyberspace should build upon the existing consensus that cyberspace is not a law-less area.[3] If States see a need to develop new rules or norms, they should build on and strengthen the existing legal framework.

In line with our mandate, we are primarily concerned with cyber operations used as means and methods of warfare during armed conflict and the protection that the law provides to the civilian population against the effects of such operations.[4] We thus urge all States to affirm that international humanitarian law (IHL) applies to cyber operations during armed conflicts, on the understanding that such affirmation neither encourages the militarization of cyberspace nor legitimizes 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

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

[2] ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2019, p. 19.

[3] See *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, 24 June 2013, para. 19; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, paras 24-25.

[4] See ICRC, *The ICRC: Its Mission and Work*, 2009.

particular the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in the other domains.

In fact, affirming that IHL applies places stringent and time-tested constraints on the cyber operations of belligerents in the unfortunate event of an armed conflict. For example, existing IHL rules strictly prohibit direct attacks against medical units and personnel, including those conducted through cyber means.[5]

Mr. Chairman,

The ICRC welcomes the discussions taking place in the context of the Open-Ended Working Group, in particular on 'how international law applies to the use of information and communications technologies by States'.[6] We encourage States to consider *how* existing IHL rules apply to cyber operations during armed conflicts.

During armed conflicts, IHL prohibits directing attacks against civilians, civilian objects and medical facilities. Does this prohibition encompass, for example, cyber operations designed to disable medical equipment or a civilian power network? Or those designed to delete social security data or civilian bank accounts?

Critical civilian infrastructure increasingly relies on digital systems and digital data have become essential for the proper functioning of government services. The answers to these questions are therefore essential for the protection of the civilian population against the effects of cyber operations. In our view, a cyber operation designed to disable a civilian network during armed conflicts would constitute a prohibited attack under IHL.

Mr. Chairman,

It is essential for States to search for common understandings on these and other questions so as to uphold in cyberspace the protection that IHL affords to civilian populations during armed conflicts.

To support governments in their deliberations, the ICRC has just submitted a position paper on *International Humanitarian Law and Cyber Operations during Armed Conflicts* to both the Open-Ended Working Group and the Group of Government Experts, in which we offer more detailed views on these issues.[7] We stand ready to lend our expertise to such discussions.

Thank you.

---

[5] 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.

[6] See UN General Assembly Resolution 73/27 (5 December 2018), para. 5.

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