Check Against Delivery

ICRC

**United Nations General Assembly**

**Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies**

**Statement by the International Committee of the Red Cross**

**Delivered by Véronique Christory, Senior Arms Control Adviser**

**15 December 2021**

Mr. Chair, Excellencies, Distinguished Delegates,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to participate in the new Open-Ended Working Group on security of and in the use of information and communications technologies. We hope that this working group will build on the landmark reports adopted by the OEWG and the GGE earlier this year.

As this is the first formal meeting of the OEWG, we would like to make two points to frame the discussion, and then respond do to some of the questions that you, Mr. Chair, posed to delegations.

Our first point is that discussions **on international law** in this **OEWG should ground in, and aim to address, today's reality**. Part of this reality is that as societies are digitalizing, so are armed conflicts. Earlier this year, the OEWG and the GGE recognized that "a number of States are developing ICT capabilities for military purposes" and that "the use of ICTs in future conflicts between States is becoming more likely."[1]

This development in military capabilities poses **new and additional threats to the civilian population**. It is today well-known that cyber operations against critical civilian infrastructure have caused significant economic harm, disruption in societies, and tension among States. The final report of the OEWG further recognized that cyber operations against critical infrastructure risk having 'potentially devastating humanitarian consequences.[2]

In light of these evolving military capabilities, and the real risk of harm to the civilian population, the OEWG should work towards **common understandings of how international law protects humans and societies against harm caused by the use of ICTs during armed conflict**.

[1] Open-Ended Working Group, Final Report, 2021, para. 16; GGE, Final Report, 2021, para. 7.
[2] Open-Ended Working Group, Final Report, 2021, para. 18.

In this respect, our second point is that this new **OEWG should be guided by the important progress achieved in the UN context over the past years**. The ICRC would like to particularly highlight the reference to international humanitarian law in the report of the Group of Governmental Experts, which noted that "international humanitarian law applies only in situations of armed conflict" and recalled "the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction". Importantly, the group underscored that "recalling these principles by no means legitimizes or encourages conflict."[3]

Mr. Chair, you have further asked which **specific rules and principles of international law applicable to State use of ICTs merit further study**. As emphasized in the Ambassador Lauber's summary of the OEWG discussions and in the GGE report, there is need for further study on "how and when" the principles of international humanitarian law apply to the use of ICTs by States.

The ICRC fully agrees with this conclusion. In our view, **developing common understandings of how and when international humanitarian law applies to cyber operations during armed conflicts, and exchanging practice of how to operationalize these legal limits, is essential to protect the civilian population. Moreover, understanding the limits that other States respect in their cyber operations can be an important confidence building measure**. In this respect, fundamental IHL rules provide a number of clear red lines. For instance,

- Direct attacks against civilian objects are prohibited, including when using cyber means or methods of warfare;
- Indiscriminate attacks are prohibited, including, for example, the employment of cyber tools that spread and cause damage indiscriminately;
- Medical services must be protected and respected, including when carrying out cyber operations.

At the same time, **the ICRC recognizes that there are other issues that need further study**, such as how the notion of civilian objects is to be understood in a digitalized world. In the study of how and when IHL applies during armed conflicts, the **ICRC calls on States to interpret – and apply – existing rules with a view to avoiding or at least minimizing incidental harm to civilians, civilian infrastructure, civilian ICT systems, and civilian data.**

Finally, Mr. Chair, you inquired about **capacity building needs** in the area of international law. The ICT environment is changing at high speed, which makes it challenging for all of use to keep track of technological, legal, policy and military developments. The ICRC is aiming to contribute to this OEWG with both technical and legal expertise on questions relating to the use of cyber operations during armed conflict, and we are also available to discuss bilaterally with interested delegations or regional groups.

Thank you.

[3] GGE, Final Report, 2021, para. 71(f).