Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

Third substantive meeting

ICRC Statement on Capacity Building

July 2022
Ambassador Gafoor, Excellencies, dear colleagues,

The ICRC is grateful for the opportunity to take part in this thematic discussion on capacity-building.

The ICRC is mandated to work for the understanding and dissemination of knowledge of international humanitarian law applicable in armed conflicts. In relation to the use of ICTs, we are implementing this mandate in several ways. Today, we would like to highlight three legal capacity-building projects that may be of particular relevance to States.

The first one is a **series of regional consultations** that we organize in partnership with States to enable dedicated exchanges among government experts on a regional basis concerning the limits that IHL imposes on cyber operations during armed conflict. Last year, we conducted such consultations first in Latin America in partnership with Mexico, and subsequently in Central and Eastern Europe in partnership with Estonia. This year, we are also looking into the possibility of convening a regional consultation in Asia. These meetings provide an opportunity for expert presentations and in-depth discussions on questions of how and when IHL applies to the use of ICTs by States. Our report on the meeting in Latin America has been published and other reports will follow. The ICRC stands ready to partner with additional States to organize consultations in other regions.

The second project we would like to highlight is the **Cyber Law Toolkit**, which the ICRC has developed in partnership with private and public institutions from China, the Czech Republic, Estonia, the UK and the US. This interactive resource is available to State representatives and other legal professionals as a self-learning and capacity-building tool. At its core are 25 hypothetical scenarios, including several which relate to the use of ICTs in the context of armed conflicts. Each scenario contains a description of cyber incidents inspired by real-world examples, accompanied by detailed legal analysis prepared and peer-reviewed by experts.

The Toolkit also offers a systematic collection of currently 30 States’ **national positions** on how international law applies to cyber operations. This collection of national positions includes a function through which all positions on a particular legal concept can be seen together. This is a practical tool for States that are developing a national position on how international law applies in the ICT
environment, or who otherwise seek to understand how other States interpret specific international law concepts in the cyber context.

Third and finally, in its role as the guardian of IHL and to support the work of States in this OEWG, the ICRC plans to publish **short notes** presenting key legal issues relating to cyber operations during armed conflicts. They will build on the position paper that the ICRC submitted to the OEWG and the GGE in 2019. The first set of these notes will address the established international legal principles of humanity, necessity, proportionality and distinction.

Thank you.