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

Third substantive meeting

ICRC Statement on International Law

July 2022
Ambassador Gafoor, excellencies, dear colleagues,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to participate in this third session of the Open-Ended Working Group. We would like to submit our main concerns and positions for your consideration in the finalization of the international law section of the annual progress report.

In her opening remarks to the second substantive session of this working group, the UN Under-Secretary-General of Disarmament Affairs reminded us of the great importance of this working group, “not despite the current challenging international security environment, but because of it.” The ICRC agrees with this assessment. Today, all States recognize that “the use of ICTs in future conflicts between States is becoming more likely”. We share this concern, and we would add that the use of ICTs in armed conflicts has – in fact – been a reality for several years, posing a real risk of harm to civilians, civilian infrastructure, and societies.

In light of this reality, we cannot over-emphasize the need for dedicated discussions on topics of international law as recommended in the chair’s draft progress report, in particular on international humanitarian law. Focused, non-politicized, and inclusive exchanges can provide a forum for States to further study how and when IHL applies – and therefore imposes limits on – the use of ICTs during armed conflict. Such discussions would by no means legitimize or encourage conflict but instead address very real humanitarian concerns.

In several recent armed conflicts, cyber operations have been conducted alongside conventional, physical warfare. There can be no doubt that these operations are subject to the long-standing rules and principles of IHL. Cyberspace is not a lawless space. Yet, States need to provide further clarity on whether the contemporary interpretations of IHL provide sufficient protection for civilians in the context of military cyber operations, or whether gaps in common understandings exist.

In our view, it would be of great concern if views prevailed that consider it lawful to disable civilian infrastructure and civilian government agencies through cyber
operations. States, should not accept claims that civilian data may be damaged or destroyed because it exists today in a digital and no longer in physical form.

Many States have raised concerns about disinformation. While information operations are not new to warfare, using ICTs to incite physical violence or cyber operations against civilians is unlawful.

As more and more individuals, private actors, and State proxies participate in armed conflicts, it is essential to reaffirm that they too must not target civilian infrastructure, and that States are responsible for all actors that operate under a State’s instructions, direction or control.

Discussions on the established international legal principles of distinction, proportionality, necessity and humanity are an important starting point. However, these principles only reflect a small part of international humanitarian law. IHL contains, among others, important rules on the imperative to protect medical facilities and on safeguarding humanitarian relief operations. Medical and humanitarian actors must be respected and protected, offline and online.

As an observer in this open-ended working group and a humanitarian organization with a mandate to ‘work for the understanding and dissemination of knowledge of international humanitarian law applicable in armed conflicts’, we are available to support States, and the Chair, in ways that are mutually agreeable. Concretely, and in relation to the draft progress report, we are available to engage in thematic discussions on international humanitarian law with a view to finding common understandings.

We will also continue to support exchanges between States and capacity-building on international humanitarian law, for instance through consultations and training courses in different regions of the world. We are especially grateful to Estonia and Mexico for having partnered with us in this work thus far.¹

Thank you.

¹ For reports of these consultations, see ICRC, Regional state consultations on international humanitarian law and cyber operations during armed conflicts, 29 June 2022.