



ICRC

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

Seventh substantive meeting

ICRC Statement on International Law

March 2024

Ambassador Gafoor, excellencies, dear colleagues,

Under your leadership, Chair, this working group has built significant agreement on ICT threats in the context of international security, including in situations of armed conflict. Delegations share a concern about ICT activities impacting the delivery of essential services to civilian populations, including medical services and humanitarian relief.

Against this background, the ICRC urges you to deepen discussions on the limits that international law, and in particular international humanitarian law imposes on the use of ICTs in situations of armed conflict. We believe progress has been achieved on this topic, and more common ground is within reach.

What convergences can we identify?

Since 2021, this group has repeatedly underscored that recalling international humanitarian law in the ICT environment by no means legitimizes or encourages armed conflicts. Delegations have rightly emphasized that international humanitarian law does not prevent armed conflicts. Indeed, international law obligations to prevent armed conflict, and to maintain peace and security, are set out in the UN Charter. IHL is different from Article 51 of the UN Charter and the right to self-defence. International humanitarian law provides limits that must be respected in the unfortunate and undesirable situation of an armed conflict, irrespective of whether the UN Charter has been violated. Today, the world faces over 120 armed conflicts, including between States. The precious humanitarian consensus that wars have limits must persist even when new means and methods of warfare are used. Your populations, the communities that delegations in this room represent, need this protection.

Discussions in this group have given an impetus to a growing number of States to express their views on the application of international law, including international humanitarian law, to the use of ICTs. The cross regional statement presented by Senegal and Colombia today, and the recently published 'Common African Position' shows that building common understanding is possible. The 55 African Union States hold unanimously that 'despite the fact that most rules of IHL emerged before the appearance of cyberspace, IHL applies [...] to cyber

operations that may be undertaken in the context of an armed conflict'. The ICRC encourages this OEWG to build on these regional and cross-regional positions, and other national positions, to include clear language on IHL in the progress report in July.

However, there also unique features of ICTs needing further discussion

However, finding agreed language on the applicability of IHL to the use of ICTs in armed conflict should not preclude discussing at the same time how IHL limits cyber operations. The need for further study on this question is reflected in the last two progress reports. In the ICRC's view, it is urgently needed.

For example, in our view it is not sufficient to simply note the principle of distinction if, at the same time, some States restrict its application in the ICT environment so much that most uses of ransomware, of wipers, or of DDoS operations are excluded because they do not result in physical damage. Interpretations of IHL that focus solely on the protection of civilian objects against physical damage are insufficient in the ICT environment.

In the ICRC's view, common understandings on the protection afforded by existing IHL can be achieved, striking the right balance between the principles of military necessity and humanity. At the same time, if existing rules of international humanitarian law are interpreted in ways that undermine the protective function of IHL in the ICT environment by leaving unaddressed the new kinds of harm resulting from the use of ICTs during armed conflict, additional rules would need to be developed to strengthen the existing legal framework and ensure it remains adequate in light of the digitalization of armed conflicts.

Thank you.