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

Second substantive meeting

ICRC Statement on International Law

March 2022
Ambassador Gafoor,

Excellencies, ladies and gentlemen,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to take the floor for a second time in this session.

Since the establishment of the first OEWG in 2019, the ICRC has repeatedly expressed concern about the growing use of cyber operations during armed conflict, their potential human cost and their disruptive effects on civilian infrastructure. These concerns are today as relevant as ever. They have been highlighted in the consensus reports of the OEWG and of the GGE and many delegations have reiterated them during the first session.

As a humanitarian organization we witness unspeakable suffering in many conflicts around the world, primarily from the use of “traditional” warfare strategies. Today, our mandate to protect civilians as well as wounded and captured soldiers requires us to also follow how cyber and other digital operations are used in times of armed conflict. We seek dialogue with States on how international humanitarian law – IHL – limits these operations.

As a matter of law and practice, and as highlighted in the 2021 GGE report, there can be no doubt: IHL applies only in situations of armed conflict. Established international legal principles and rules protecting civilians and combatants hors de combat impose essential limits on the conduct of cyber operations:

- The principle of distinction prohibits cyber attacks directed against civilian objects – such as hospitals, critical civilian infrastructure and civilian public administrations;
- The principle of proportionality prohibits attacks – including cyber attacks – which may be expected to cause excessive incidental harm to civilians and civilian infrastructure. Especially in cyberspace, incidental harm risk being widespread and transcend national borders.
These rules apply to State armed forces, other State agents, non-state armed groups, but also to those who directly participate in hostilities during an armed conflict, including volunteer hackers and other civilians.

Mr Chair, you posed two questions to delegations, one relating to capacity building, and one on sharing national views and building common understandings. In our view, these questions are closely related.

We believe that the ongoing exchanges in this OEWG and the publication by States of national views on the application of international law are as such an important element of capacity building. The OEWG provides a forum for exchange and discussion among all States on ‘how’ and ‘when’ IHL applies to the use of ICTs by States, and it should build on the important progress made in the first OEWG and the GGEs over the past years. We hope that the coming sessions will enter into further detail on the law and facilitate dialogue, thereby strengthening mutual understanding among all States. The ICRC is ready to lend its expertise to such discussions.

A number of States have also published national views on how international law applies in the information environment. These publications provide a unique source of official views on international law that all States can consult and consider when forming their own views on the subject. To facilitate access to these views, in partnership with several private and public institutions around the world – from China, the Czech Republic, Estonia, the UK and the US – the ICRC is offering a Cyberlaw Toolkit. Among other things, the Toolkit presents all national views of States and provides a function through which all views on a particular subject can be seen together.

These national views should inform discussions in the OEWG on how and when international law, including IHL, applies to cyber operations. National views published to date present convergence towards shared understandings on several issues. In its role as guardian of IHL, the ICRC plans to publish short notes explaining key legal issues relating to cyber operations during armed conflicts, which we hope will support States when drafting national positions, inform the discussions of this Group, and help finding common ground.
Finally, the Open-Ended Working Group provides a global and unique forum to present work conducted by States in different regions. For example, in the session last December, Mexico and Estonia reported that they conducted regional consultations – in partnership with the ICRC – to enable in-depth discussion among government experts on cyber operations during armed conflict. We hope that the forthcoming reports from these consultations will be informative for all States. The ICRC stands ready to partner with other States to organize additional consultations in other regions of the world.

Thank you.