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

Second substantive meeting

ICRC Statement on Existing and Potential Threats in the Sphere of Information Security

March 2022
Ambassador Gafoor,

Excellencies, ladies and gentlemen,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to participate in the second session of the Open-Ended Working Group on security of and in the use of information and communications technologies.

We take the floor in this segment on existing and potential threats to alert delegations to a growing threat of cyber operations against humanitarian organizations. We call on you, States, to take cooperative measures to prevent such threats and to ensure that humanitarian organizations are protected online as they are offline.

Since the beginning of 2022, the ICRC has been the victim of several hostile cyber operations. Most concerningly, in January we discovered that servers hosting the personal information of more than 500,000 people who receive humanitarian services from the Red Cross and Red Crescent Movement were compromised. While this is a shock, it was not a unique occurrence. Over the past years, several international and humanitarian organizations have been the victim of hostile cyber operations.

If cyber operations target humanitarian organizations, they risk causing severe consequences for the people we serve. Concretely, the cyber operation against our servers breached personal data of missing people and their families, of unaccompanied or separated children, of detainees, of migrants, and of other people receiving humanitarian services. If in the wrong hands, this data can be misused to harm particularly vulnerable people. Moreover, the recent data breach forced us to take the compromised systems offline, severely limiting our humanitarian services during this period. Every day the Red Cross and Red Crescent Movement helps reunite 12 people with their families – and thus every day during which these activities are disrupted prolongs their distress.
Cyber operations also undermine the trust of people and parties to armed conflicts that we depend on, which in turn affects our operations in humanitarian emergencies. A loss of trust can also pose risks to the security of our staff.

Digital threats to humanitarian organizations risks unsettling a long-standing consensus on the need for and protection of impartial humanitarian activities. The services provided by the ICRC, the wider Red Cross and Red Crescent Movement, and of other humanitarian organizations are critical for vulnerable people and accepted by States and parties to armed conflicts. For example, the Geneva Conventions and our Movement Statutes – which are agreed to by all States – mandate the ICRC to assist and to protect persons affected by armed conflict and other situations of violence. This global consensus on humanitarian action must prevail in the digital age.

For several years, the ICRC has emphasized the imperative that humanitarian data and digital infrastructure be protected against digital threats. We have recalled that international humanitarian law requires all parties to armed conflicts to allow and facilitate humanitarian activities, and that humanitarian staff and relief consignments must be respected and protected. Such protection is not only needed in contexts of armed conflict – it is also essential during natural disasters and other emergencies. Humanitarian action needs protection, in the physical world and in the global information environment. As States in the Group of Friends of the Protection of the Civilian Population put it aptly:

“The trust of the people they serve is the currency of humanitarian organizations. This trust is a precondition for humanitarian action. Therefore, we, as Members States, must create an environment, including a safe information infrastructure that allows humanitarian organizations to successfully carry out their mandate.”

We urgently call on you, the States, to reaffirm that humanitarian organizations, their staff, and humanitarian data must never be targeted, be it in the physical or in the digital world. We are seeking a conversation to ensure that the international legal and other normative frameworks adequately protect humanitarian organizations from the negative secondary effects of the digital
transformation. And we also invite you to support efforts of the humanitarian community to ensure the best possible protection against digital threats. We need your help, and we need the help of tech companies, academia, and other experts. We cannot do this alone – it is our collective responsibility.

Thank you.