Comments by the International Committee of the Red Cross on the Initial “Pre-draft” of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

The International Committee of the Red Cross (ICRC) has studied the 'Initial “Pre-draft” of the report of the OEWG on developments in the field of information and telecommunications in the context of international security' with great interest and wishes to commend the Chair, his Excellency Ambassador Lauber, and his team for the high quality of this initial pre-draft.

The ICRC would like to submit to you and to the attention of all States taking part in the OEWG the following comments.

Section B: Existing and Potential Threats

The ICRC would encourage the Chair to consider mentioning additional critical civilian infrastructure sectors that may be threatened by the use of ICTs (para. 19). While a list of critical infrastructure cannot be exhaustive, the ICRC believes that emphasizing the threat against infrastructure that enables the delivery of essential services to the population is important.

The ICRC strongly supports explicit mentioning of the health care sector in the report (para. 19), which indeed is particularly vulnerable to cyber attacks. In addition, the ICRC would like to emphasize the importance of electrical, water, and sanitation facilities, which form the backbone of essential services for the population. This infrastructure is often operated by industrial control systems. The frequency of cyber attacks against such systems is reportedly increasing and the severity of the threat has evolved more rapidly than anticipated only a few years ago.

Thus, the ICRC encourages the OEWG to explicitly mention in the report the threats that cyber operations may pose to the delivery of such essential services to the civilian population.
Section C: International Law

The ICRC commends the Chair for carefully reflecting the discussions of States in the first two substantial meetings of the OEWG in this section of the report.

The ICRC believes that it is of great importance to underscore in the report that ‘international humanitarian law reduces risks and potential harm to both civilians and combatants in the context of an armed conflict’ (para. 25). Indeed, international humanitarian law aims to protect the victims of armed conflict by restricting permissible means and methods of warfare.

Similarly, the ICRC would welcome if the report will recall that ‘international humanitarian law neither encourages militarization nor legitimizes conflict in any domain’ (para. 25). It may be noted in this respect that States had found agreement on this point when adopting by consensus the preamble to the 1977 First Additional Protocol to the 1949 Four Geneva Conventions, in which States parties expressed ‘their conviction that nothing in this Protocol or in the Geneva Conventions of 12 August 1949 can be construed as legitimizing or authorizing any act of aggression or any other use of force inconsistent with the Charter of the United Nations’. The ICRC calls on States not to fall behind this consensus.

The ICRC agrees with the Chair that ‘certain questions on how international law applies in the use of ICTs have yet to be fully clarified’ (para. 27). As underscored in its statements and position paper on ‘International Humanitarian Law and Cyber Operations during Armed Conflicts’ (part V, pp. 6-9), the ICRC is conscious that States have different views on the interpretation of certain IHL rules and principles.

The ICRC would suggest including reference to the principles of ‘humanity, necessity, proportionality and distinction’ in the report, either in addition to or instead of ‘the protection of civilians and civilian objects’. This would build on the 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, where these principles had been ‘noted … where applicable’ (para. 28(d)). They are also more commonly referred to as ‘principles of IHL' and share the objectives of protecting civilians and civilian objects.

In this respect, the ICRC would further recommend adding reference to the principle of precautions. Taking all feasible precautions to avoid or at least minimize incidental civilian harm when carrying out attacks is of utmost importance in cyberspace, where attacks risk to spread easily and cause widespread harm to civilian objects (position paper on ‘International Humanitarian Law and Cyber Operations during Armed Conflicts’, part IV, pp. 5-6).
Section D: Rules, Norms and Principles for Responsible State Behaviour

The ICRC welcomes that the report recalls States’ suggestions for the further elaboration of norms, including that ‘States should not conduct ICT operations intended to …harm medical facilities’ (para. 38). The ICRC is indeed concerned about the particular vulnerability of the health-care sector to cyber attacks. This risk is acute at all times – it is even more dangerous in times of conflict or pandemics.

If States decide to further elaborate certain norms, the ICRC would like to recall its proposal of a possible new norm, which could state: ‘States should not conduct or knowingly support ICT activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm.”