Statement of Canada

Workstream 6: Upholding International Humanitarian Law in the Use of Information and Communication Technologies During Armed Conflicts

3rd Round of Consultations

Sessions 1 and 2

Session 1

Mr. Co-Chair, Madam Co-Chair, Canada appreciates the dedicated work that created the concept note for this third consultation. Since last June, you have been guiding us through important discussions that bring us together.

We deeply care about the product that will stem from these discussions, and our comments are anchored in the will of being constructive in our contribution to make your task easier.

For this first session, allow me to start with broader comments, which will be followed by more specific ones.

Canada welcomes the key recommendation that the principles of humanity and military necessity are applicable in the cyber context and play a key role in concrete application of IHL to govern cyber operations.

Canada agrees that the principles of distinction, proportionality and precaution apply to attacks conducted by cyber means.

We would add that harmony across the recommendations will be key as we navigate our way to common understandings.

For this and in line with resolution 34IC/24/R2, we would welcome differentiating malicious ICT activities wherever possible in the recommendations. This distinction is needed to distinguish malicious use from regular and even positive uses of cyber to ensure IHL compliance. I will speak more to this the second session.

Canada would find useful for the recommendation to follow the structure of the objectives and clearly distinguish between the legal interpretation of the rules, from encouraged best practices from a policy perspective, as well as the areas for further discussions. Our interventions today will focus on the legal interpretation.

On the definition of attack, we consider that there remains a diversity of opinion as to whether the mere act of disabling amounts to an attack under IHL. Canada considers that a cyber operation will qualify as an attack when the effects of the cyber operation must *reasonably be expected to cause* injury or death to persons or damage or destruction to objects. This requires violence. As just mentioned, it is important that the recommendations reflect both common understandings and the need for further discussions from States.

On the protection of data, we find useful the approach taken to discuss different rules which could be relevant when a cyber operations conducted in the context of an armed conflict may affect or target data. However, we are concerned that the discussion as framed still presupposes that data is an object for the purpose of IHL. Yet, the recommendation should not favour one interpretation over another. For example, to qualify data as a military objective, one would need to presuppose that the question is resolved, which is not the case. We feel strongly that key conclusions should reflect the current debates as to how data is classified for the purpose of IHL.

Canada agrees that a party to an armed conflict must take all feasible precautions in the choice of means and methods of attack to avoid or at least minimize death or injury to civilians and damage or destruction to civilian objects. This obligation applies in cyberspace.

However, we disagree with the characterization of this rule as requiring attacks to "affect only the components or functions of ICT infrastructure used for military purposes and not those serving civilian purposes". Instead, the existing IHL rules for identifying military objectives should be applied.

As mentioned, previously, it is our view that an assessment of a cyber operation's legality would not include the notion of *reverberating effects*. We would encourage keeping language closer to the law: "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof".

We agree that careful attention needs to be paid to the implementation of States' obligations related to IHL dissemination when the physical distance from an armed conflict no longer limits who can take part in it. This obligation should be formulated with article 83 AP1 language.

Session 2

Canada concurs that medical personnel, units and transports, as well as humanitarian personnel and objects, must be respected and protected at all times, in accordance with IHL, including against the effects of **malicious** cyber activities.

However, the observations provided about the content of this obligation need to align with existing law.

We object to the idea that parties to an armed conflict have an obligation to "take feasible measures to prevent medical services and humanitarian activities from being harmed, including through ICT activities *by third parties* such as cyber criminals and other non-state actors not attributable to a party to an armed conflict". These third parties could be located in the territory and jurisdiction of a non-belligerent. Parties to an armed conflict have no obligation to intervene in domestic law enforcement activities of a non-belligerent.

Canada remains interested in learning more about the research conducted by the ICRC on a possible digital emblem, as articulated in our support for the IC 34 Resolution on ICTs. We appreciate the ongoing dialogue between the ICRC and States on that project, which now goes back to several years. We encourage the ICRC to continue consulting and actively engaging with States on that important project of which we still require further understanding.

Whether information is disseminated through ICTs or through physical means, the applicable law remains the same. For instance, the prohibition to incite violations of IHL applies to the cyber context. We would encourage that the language here does not overstates the obligations.

On the implementation of our understanding of IHL as it applies to cyber, Canada is glad to speak to how the technological developments are enabling our operators, including cyber-operators, to comply with IHL. Within the Canadian Armed Forces, ICTs enable and amplify the ability to respect key IHL obligations.

The Directorate of Cyber Operations Law's primary role is to provide legal advice and training to the Canadian Armed Forces Cyber Command in their conduct of cyber operations. There is an important nuance to be made however, which is that these legal advisors are not using *lex specialis* in their advice, but the same LOAC rules that are applicable in any military operation.

There are other agencies conducting cyber operations for Canada, and each of them has their own dedicated legal counsel embedded into their operational cycles and governance framework. Our commitment to promoting and abiding by IHL in cyberspace has very concrete implications.