Talking points

ICRC Global Initiative – Workstream 6: Use of ICTs during armed conflict

Thursday, 15 May 2025

CHECK AGAINST DELIVERY

Session 1: The Use of ICTs in today's armed conflict and the human cost

Introductory remark and general comments

Before diving in and addressing the topic of the first session, let me start of by congratulating the ICRC in setting up this global initiative. Importantly, we are pleased that within this process a workstream is dedicated specifically to the use of ICTs during armed conflict.

We also congratulate the Chairs of this workstream for all the preparatory work that went into this meeting.

The background paper is thought provoking and addresses novel ideas. Canada is grateful for the opportunity to participate to this consultation. We see today's meeting as a great opportunity to help identify priority issues and areas of convergence.

Canada is a fervent champion of the Rules Based International Order and is committed to following and promoting the application of international law, including International Humanitarian Law (IHL) or the Law of Armed Conflict (LOAC) in cyberspace. This topic is one of great importance to us.

Over the past decade, Canada has been championing, supporting and participating in discussions on how international law, including IHL, applies in cyberspace. There has been a growing momentum on this topic and great progress made in this area.

There has been immense work put towards building common understandings on how international law applies to cyberspace. This notably happened at the United Nations *Open-Ended Working Group on security of and in the use of information and communications technologies* (OEWG). As noted in the background paper, multiple States and Regional Organizations have developed a national position on international law and cyberspace. Canada published its own position in 2022, and Canada is proud to have contributed to and been involve in many capacity building initiatives to assist others in doing the same.

Another great example of momentum and building common understanding is certainly the recently adopted *Resolution on 'Protecting civilians and other protected persons and*

objects against the potential human cost of ICT activities during armed conflict' which Canada supported and hope to see language on in the final report of the OEWG.

In relation to the present meeting and as a general comment, Canada's experience has been that a helpful approach taken when building common understandings has been to get involve in concrete and practical discussions grounded in the law. We would suggest that the work of this group would likewise benefit from this type of approach, discussing the applicable international rules first and then applying them to practical scenarios.

Question 4: What measures has your state taken to assess or mitigate the human cost of ICTs activities during armed conflict? Are there lessons learned that you could share with other delegation?

Turning to heart of the matter, thank you to Mr. Mauro Vignati for the excellent presentation.

It is not feasible to address all guiding questions suggestion for each session, but for this session we will focus on question 4.

We note from the background paper the acknowledgment of the advantages of relying on ICTs in conflict affected areas, and the vulnerabilities and risks it creates. An advantage which is alluded to in the paper, but is worth emphasizing, is the technological developments enabling operators, including cyber-operators, to get it right. ICTs enable and amplify the ability to respect key IHL obligations. For example, for the principle of 'distinction', operators are able to use technology to distinguish between military objectives and civilian objects on the battlefield. We see it indispensable for our cyber-operators to have tools at their disposal to enhance their ability to comply with IHL.

This is what Canada deeply cares about. This is why, for example, Canada's Office of the Judge Advocate General has a Directorate of Cyber Operations Law, staffed with legal advisors. Their primary role is to provide legal advice and training to the Canadian Armed Forces Cyber Command in their conduct of cyber operations. It was the Commander of the Cyber Command who advocated to make sure the Cyber Command had dedicated legal advisors, demonstrating the commitment that the military chain of command places on conducting cyber operations in accordance with Canada's legal obligations.

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

Session 2: Protecting civilians and other protected persons and objects from the dangers arising from ICT activities during armed conflict.

[Thank presenter, Professor Heather Harrison Dinniss]

Building on my earlier intervention, Canada regards IHL to be a comprehensive body of law that has stood the test of time and is capable of responding to the new realities of contemporary warfare. IHL protections are applicable not only in the conventional domain, but also in the cyber domain, and can be meaningful in mitigating against the risks created by the unlawful use of ICTs during armed conflict.

We noted that the Paper sometimes suggests going beyond the current interpretation of the law to respond to the new realities of contemporary warfare and suggest that we should collectively expand the interpretation of the law. We will simply note here that there is always a risk in developing a new interpretation of the law. It can inadvertently harm or degrade the protections already provided by it.

Canada has found it helpful to issue our National Position on International Law Applicable in Cyberspace to promote clarity and consistency in the application of the law related to ICTs. It enables legal advisors within the government of Canada to give appropriate advice across government and to cyber-operators who are conducting activities in armed conflict.

When issuing our national position on international law and cyberspace Canada provided its interpretation of the notion of "attack" as follows: "cyber activities, whether in offence or defence, where their effects are reasonably expected to cause injury or death to persons or damage or destruction to objects". This could include harmful effects above a *de minimis* threshold on cyber infrastructure, or the systems that rely on it.

A side note on this, Canada has not included the idea of "reverberating effects" in our National Position on International Law Applicable in Cyberspace and wonder whether it can appropriately be labeled as "widely accepted" as a legal principle.

Now coming back to the notion of cyber attacks, they must respect relevant treaty and customary IHL rules applicable to attacks. This includes those relating to distinction, proportionality, and the requirement to take precautions in attack. These obligations arise at the point of launching an attack. When assessing compliance with these obligations, the factors taken into consideration are focused on intent rather than effects. For example, the degree of impact of an attack (e.g. numbers of civilians injured) does not yield a conclusion in and of itself about the lawfulness of the attack.

As you know, Canada, like most other States, has not adopted the position that data is an object under IHL. While we are giving this issue due consideration, as of now, we don't see this characterization as part of the international law corpus.

What we acknowledge as an integral and important part of IHL is the protection afforded to medical personnel, units and transport. These protections like all others apply to cyberspace. Canada was and remains interested in learning more on 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.

Session 3: Protecting civilians and other protected persons from information spread in violation of IHL during armed conflict

[Thank presenter, Professor Martha M. Bradley]. We take this occasion to recognize and acknowledge your important role in the development of the Common Position of the African Union. Canda was honored to work the AU Member States in reaching a common position. We consider very important to hear African voices in this ICRC-lead process.

Canada believes that compliance with existing IHL is the appropriate anchor for all discussions related to ICT activities in armed conflict. We thus recognise the value in considering how existing IHL obligations might apply to ICT activities that harm civilians or other protected persons. However, Canada is sensitive to efforts to imbue these obligations with expanded meaning to address perceived gaps in the law. For example, we would not agree that Common Article 1 to the Geneva Conventions contains a prohibition against the encouragement or incitement of IHL violations by digital means. Instead, we are of the view that Common Article 1 requires High Contracting Parties to respect and ensure respect for the obligations in the Conventions by people within their jurisdiction and control.

In this regard, Canada unfailingly respect, and ensures respect, for the Geneva Conventions and for broader IHL. We have a strong and active national humanitarian law committee, we engage actively in public training, outreach and advocacy, and we have robust training programs for members of the Canadian Armed Forces. Impunity for IHL violations is not tolerated.

Session 4: the risk of harm arising from the military use of civilian ICT infrastructure and the involvement of civilians in ICT activities during armed conflict.

[Thank presenter, Professor Lijian Zhu]

I will remain brief for my last intervention.

Regarding the military use of civilian ICT infrastructure and the resulting impact on its protection under IHL, we do not consider the non-legal concept of “dual use” as relevant to our legal analysis. Instead, the definition of “military objective” in Additional Protocol I

provides the necessary characterization of what qualifies as such – whether in cyberspace or in other domains. It is our position that cyber attacks are governed by the same rules and limitations governing conventional attacks. Cyber attacks must respect relevant treaty and customary IHL rules applicable to attacks including those relating to distinction, proportionality, and the requirement to take precautions in attack.

I also take the opportunity to thank you Mr./Ms. Chair for leading this meeting throughout the day. We will reflect on the insightful discussions and ideas that were circulated today and continue our efforts to reinforce the applicability of IHL in cyberspace. We look forward to the progress reports and the meeting in October.

DATE: 2025-05-15