ICRC Global Initiative to Galvanize Political Commitment to International Humanitarian Law

Workstream 6: Upholding IHL in the Use of Information and Communication Technologies during Armed Conflicts

Second State Consultation

Statement of Australia – Session 3

24 November 2025

Good afternoon colleagues.

Australia welcomes the opportunity to contribute to this important discussion on operationalising specific protections for persons, objects and activities against the effects of the use of ICTs during armed conflict.

We thank the panellists for their excellent insights. We also thank the ICRC and co-chairs for the background paper, which thoughtfully raises, among other issues, the question of whether data can constitute an object under IHL. States' views appear to be varied, and we look forward to continuing discussions on this important subject.

What is clear is that while it remains unsettled whether data can constitute an object under IHL, certain data is already protected under IHL by virtue of being an essential part of the functioning of a protected facility or operation.

Australia recognises that in the digital age, the data held by medical and humanitarian organisations – including patient records, logistics systems, and communications – is integral to the delivery of care and assistance to civilians in need.

IHL provides special protection to medical units and requires that medical units and transports be respected and protected at all times. IHL also imposes obligations to respect and protect humanitarian personnel, and to allow and facilitate rapid and unimpeded humanitarian relief for civilians in need.

These protections extend not only to the personnel of such organisations but also to the systems and data that enable their operations.

Accordingly, parties to an armed conflict should respect and protect these organisations when conducting cyber operations.

We do not consider that all cyber operations in respect of medical and humanitarian organisations would amount to a violation of IHL. For example, it may not be unlawful to conduct non-damaging cyber reconnaissance to determine whether a medical facility is being used to commit hostile acts outside its humanitarian functions.[1]

As we have detailed, Australia considers that the data of medical and humanitarian organisations is already protected by the application of existing IHL rules and principles. In our system, trained legal officers advise commanders and staff prior to any cyber operation that may affect ICT services, cyber infrastructure or data essential to the operation or administration of medical or humanitarian organisations, to ensure compliance with Australia's obligations under IHL and domestic law. We call on all parties to an armed conflict to adhere to their obligations concerning the protection of medical and humanitarian organisations when conducting cyber operations.

Thank you.

[1] Example raised in Tallinn Manual, rule 132, paragraph 2.

ICRC Global Initiative to Galvanize Political Commitment to International Humanitarian Law

Workstream 6: Upholding IHL in the Use of Information and Communication Technologies during Armed Conflicts

Second State Consultation

Statement of Australia – Session 4

24 November 2025

Australia welcomes the opportunity to address the safeguarding of civilians and other protected persons from information spread in violation of IHL during armed conflicts.

On the first guiding question, the third Geneva Convention is clear that exposing POWs to insults and public curiosity is prohibited. The protection of POWs from public curiosity, including in mediums such as newspapers and television, is not a new concept; however, the proliferation of newer forms of media, such as social media and messaging applications, have made information spread in violation of IHL quicker and easier to disseminate.

In Australia's view, the online publication of content such as images or videos by a party to an armed conflict that identifies or humiliates POWs may amount to a violation of IHL, as such publication may subject POWs to public curiosity. It is important that detaining powers comply with their obligations and treat POWs humanely. Australia also urges media organisations and individuals to exercise caution and sensitivity when handling content involving POWs.

With respect to the second guiding question, Australia recognises the growing threat posed by disinformation campaigns that incite or encourage violations of IHL. In order to counter such disinformation campaigns, the Australian Defence Force (ADF) requires its commanders and staff to always assess information carefully by considering its relevance, accuracy, timeliness, usability, completeness and precision. This criteria assists the ADF with combating disinformation campaigns that incite IHL violations, including against medical and humanitarian personnel.

The scenario posed in this question considers an online campaign, where fabricated images falsely claim a hospital is a combatant stronghold. If such a campaign incited IHL violations – for example,

by encouraging attacks on protected facilities by falsely claiming they were a combatant base – there may be a violation of IHL.

Such a campaign may also breach the prohibition on "acts or threats of violence, the primary purpose of which is to spread terror among the civilian population". The speed and ease at which content can be shared and disseminated throughout a population means such campaigns can quickly terrorise a civilian population.

Not all online campaigns will violate IHL. However, parties to a conflict must ensure that their information operations respect the legal limits imposed by IHL and international human rights law.

Finally, we recognise the impact that the spread of misinformation and disinformation may have on humanitarian organisations, including disrupting humanitarian activities, undermining trust in their work, and threatening the safety and security of their personnel.

Australia was proud to work with a Ministerial Group in developing the Declaration for the Protection of Humanitarian Personnel, which more than 100 States have endorsed.

Signatories have committed to countering misinformation and combatting disinformation, information manipulation and hate speech targeting humanitarian organisations, personnel and activities. Signatories have also committed to actively de-politicise humanitarian action, including by building understanding with local authorities and the media, protecting the independence of journalists, and raising awareness and calling out actors that perpetuate disinformation and hate speech. The Declaration recognises that we must work with technology companies to support these efforts.

In closing, Australia affirms that cyber operations in armed conflict must be conducted in accordance with IHL.

Thank you.