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

Third State Consultations

Statement of Australia

16 February 2026

Australia would like to thank the ICRC and co-chairs for their efforts throughout this process. These consultations have highlighted where States share common understandings, and where there is opportunity for further discussion.

Australia agrees that it is essential to uphold and reinforce respect for international humanitarian law (IHL) in the conduct of cyber activities during armed conflict. The use of cyber capabilities does not change the fact that all parties to armed conflict must comply with their legal obligations under IHL.

States agree on the legal rules governing attacks during armed conflict. These rules apply to all mediums of attack, whether kinetic or cyber in nature. A cyber activity may constitute an 'attack' if it rises to the same threshold as that of a kinetic 'attack'. Accordingly, in Australia's view, a cyber activity that results in the reasonably foreseeable death or injury to individuals, or damage and destruction to objects, would amount to an attack under IHL.

However, Australia considers further discussion is required amongst States on the question of whether a cyber activity that merely disables an object would amount to an attack under IHL, as there is currently no settled consensus on the issue.

In assessing the incidental effects on civilians and civilian objects arising from attacks on cyber infrastructure that constitutes a military objective, Australia recalls that Additional Protocol I requires consideration of expected incidental loss of civilian life, injury to civilians, and/or damage to civilian objects. Australia does not support substituting this established legal standard with broader formulations such as "*all foreseeable direct and indirect effects*," which risk introducing legal and decision-making uncertainty, and depart from the text and object of existing law.

The concept note refers to an observation made by the co-chairs and the ICRC that States must exercise due diligence to prevent violations of IHL committed by civilians through, or facilitated by, cyber activities and must suppress such violations if they occur. We understand this to be an interpretation derived from the obligation on States to 'ensure respect' found in Common Article 1 to the Geneva Conventions.

Australia considers the phrase 'ensure respect…in all circumstances' refers to obligations on a State to ensure respect by their armed forces and other persons or groups whose conduct is attributable to that State under the rules on State responsibility.

Co-chairs, the concept note underscores the significant human consequences that cyber activities during armed conflict may generate. Australia agrees with these observations, but we would also like to highlight the ways in which the lawful use of cyber capabilities may enhance States' compliance with IHL.

Cyber capabilities may improve situational awareness through real-time intelligence, surveillance, and reconnaissance. In some cases, cyber-enabled effects may offer greater protections than kinetic alternatives through enhanced precision, reversibility and scalability, with the potential to reduce incidental civilian harm and, where feasible, avoid escalation.

At the operational level, networked command-and-control and data link capabilities combined with Intelligence Surveillance and Reconnaissance platforms can enable real-time situational awareness across air, maritime, and joint environments. This can improve the accuracy and timeliness of information, strengthening the ability of commanders to adhere to IHL through more informed decision-making.

Cyber capabilities can also support legal oversight and accountability in military operations in armed conflict. Targeting processes are supported by secure digital systems that integrate intelligence, collateral damage estimates, and advice from embedded legal advisers, while protected networks enable the rapid dissemination of up-to-date rules of engagement and legal guidance to deployed forces.

Co-chairs, Australia thanks you for the opportunity to discuss this important dimension of armed conflict.