



Power of humanity

34th International Conference
of the Red Cross and Red Crescent

28–31 October 2024, Geneva

Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict

DRAFT RESOLUTION

September 2024

EN

34IC/24/9.2DR
Original: English
For decision

DRAFT RESOLUTION

**Protecting civilians and other protected persons
and objects against the potential human cost of
ICT activities during armed conflict**

The 34th International Conference of the Red Cross and Red Crescent (International Conference),

recognizing that an increasingly digitalized and connected world provides opportunities in the social, economic, development, humanitarian, and information and communication spheres, and can help save and improve lives, including in situations of armed conflict,

underlining the importance of connectivity and information and communications technologies (ICTs) for the delivery of essential goods and services – including food, water, electricity, heating, sanitation, as well as medical and humanitarian services – to civilian populations and other protected persons, and for civilians to seek and receive information in an accessible format about where to find safety and objects essential for their survival and how to maintain family contact, including in situations of armed conflict,

recalling that the use of ICTs in future conflicts between States is becoming more likely, and *noting* that ICTs, including ICT-enabled information operations, have already been used in armed conflicts in different regions,

expressing concern that the use of ICT capabilities by parties to armed conflicts may cause harm to the civilian population and other protected persons and objects, including across international borders, in particular where directed against, or incidentally affecting, ICTs that are part of civilian objects, including civilian critical infrastructure and essential services, or works and installations containing dangerous forces,

expressing further concern that a lack of adequate capacities to detect and defend against malicious ICT activities may make States and components of the International Red Cross and Red Crescent Movement (Movement) more vulnerable,

expressing concern about the scale, speed and reach of disinformation, hate speech and other harmful information spread through ICTs, in particular social media platforms, and the risks of harm that such use of ICTs can cause to the civilian population and other protected persons during armed conflict, including when used to recruit children into armed forces,

recognizing that all persons, including women, men, girls and boys of different ages, disabilities and backgrounds, can be affected differently by ICT activities,

noting with concern that the use of artificial intelligence and other emerging technologies in malicious ICT activities may further increase their scale and speed, as well as the harm they may cause,

noting that ICTs enable or are used to encourage civilians to conduct or support ICT activities in armed conflict, and *expressing concern* that civilians may not be aware of the risks involved or the legal limits applicable to their conduct,

recalling that private technology companies provide a range of ICT products, services and infrastructure on which civilian populations, governments and humanitarian organizations rely, including during armed conflict, and *underlining* the importance of the availability of these products, services and infrastructure for civilian populations,

recognizing that ICTs are essential for efficient and effective humanitarian operations, and *expressing* deep concern about the impact that ICT activities have on humanitarian organizations, including data breaches and disinformation that target them, disrupting their relief operations, undermining trust in humanitarian organizations, including Movement components, and threatening the safety and security of their personnel, premises and assets, and ultimately their access and ability to carry out humanitarian activities,

recalling the legal and protective value of the distinctive emblems and signals, and *expressing interest* in the ongoing research on the purpose, parameters and feasibility of a digital emblem conducted by the International Committee of the Red Cross (ICRC), in collaboration with academic institutions and other Movement components,

reaffirming Resolution 4, “Restoring Family Links while respecting privacy, including as it relates to personal data protection”, adopted by the 33rd International Conference, and *emphasizing* that the issues addressed in that resolution are also important for the protection of other humanitarian data,

taking note of Resolution 12, “Safeguarding humanitarian data”, adopted by the 2022 Council of Delegates, *welcoming* the Movement’s commitments on the protection of their humanitarian data, including on strengthening capacities, and *emphasizing* the importance of the confidentiality, integrity and availability of data for humanitarian operations,

taking note also of United Nations General Assembly Resolution 76/19 and the work by States in the United Nations open-ended working group on security of and in the use of information and communications technologies 2021–2025,

calling on States to avoid and refrain from taking any measures not in accordance with international law in their use of ICTs, in particular the Charter of the United Nations, including the obligation to settle international disputes by peaceful means and the prohibition of the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations, *reaffirming* the conviction that nothing in international humanitarian law (IHL) can be construed as legitimizing or authorizing any act of aggression or any other use of force, and *emphasizing* that recalling IHL by no means legitimizes or encourages conflict,

recognizing that the specificities of the ICT environment raise questions on how certain principles and rules of IHL apply in situations of armed conflict and that States have taken diverse views on such questions,

emphasizing that people and critical infrastructure, as well as medical and humanitarian organizations, risk facing harm caused by ICT activities at all times, *calling on* States to build on this resolution to take effective measures for their protection in line with applicable legal frameworks and their current ICT capacities, and *asking* the Movement to take appropriate ICT security and data protection measures at all times,

1. *expresses* the shared commitment of all members of the International Conference to protect the civilian population and other protected persons and objects in situations of armed conflict, including against the dangers arising from ICT activities;
2. *recalls* that IHL applies only to situations of armed conflict – including the established international legal principles of humanity, necessity, proportionality and distinction –

and in armed conflict applies only to conduct that takes place in the context of and is associated with that conflict;

3. *recognizes* the need for further study on how and when these principles apply to the use of ICTs, *underscores* that recalling these principles by no means legitimizes or encourages conflict, and *urges* States to find common understanding in this respect, while noting the possibility of the future elaboration of additional binding obligations, if appropriate;
4. *reiterates* that, in situations of armed conflict, IHL rules and principles – including the principle of distinction, the prohibition of indiscriminate and disproportionate attacks, the obligations to take constant care to spare the civilian population, civilians and civilian objects in the conduct of military operations, and to take all feasible precautions to avoid, and in any event minimize, incidental civilian harm, the prohibition of encouraging or inciting violations of IHL, and the prohibition of acts or threats of violence, the primary purpose of which is to spread terror among the civilian population – serve to protect civilian populations and other protected persons and objects, including against the dangers arising from ICT activities;
5. *calls* on parties to armed conflicts to ensure, in accordance with their international legal obligations, the protection of critical infrastructure that provides services across several States, such as the technical infrastructure essential to the general availability or integrity of the internet, including undersea cables and orbit communication networks;
6. *also calls on* parties to armed conflicts to respect and protect medical personnel, units and transports in accordance with their international legal obligations, including with regard to ICT activities;
7. *calls on* States and parties to armed conflicts to allow and facilitate impartial humanitarian activities during armed conflict, including those that rely on ICTs, and to respect and protect humanitarian personnel and objects in accordance with their international legal obligations, including with regard to ICT activities;
8. *urges* States and parties to armed conflicts to effectively protect civilian populations and other protected persons and objects in accordance with their international legal obligations, including with regard to ICT activities;
9. *calls on* States, as well as Movement components as appropriate and in accordance with their respective mandates, to disseminate knowledge of IHL as widely as possible in their respective countries, so that the principles thereof may become known to the entire population, *urges* States to take measures to prevent IHL violations, and *recalls* States' commitment to take measures necessary for the suppression of IHL violations, including through investigation and prosecution where appropriate;
10. *encourages* all Movement components to consider the risk of harm that may be caused by ICT activities to the civilian population and other protected persons and objects, *urges* all Movement components to improve their preparedness for and ability to respond to the risks of such activities, including how different groups of people may be harmed in different ways, for example by building capacities to detect such risks and prevent harm for civilian populations, and *invites* States to support the Movement in these endeavours;
11. *encourages* States, as well as Movement components as appropriate and in accordance with their respective mandates, to take measures to make private technology companies within their jurisdiction aware that providing ICT services to clients that are or may become involved in armed conflict involves certain risks and to

engage, as appropriate, with these companies to encourage them to further inform themselves of these risks and to adopt, when necessary, measures that inform staff about and protect staff from such risks and enable them to act in a manner that is consistent with the applicable law;

12. *encourages* the ICRC to continue consulting and actively engaging with States and Movement components to further assess and clarify the specific purpose and technical feasibility of a digital emblem, to provide, where feasible, capacity-building to interested Movement components and States on its potential use in relation to armed conflict, and to explore possible legal and diplomatic avenues in this respect;
13. *calls on* Movement components to take appropriate steps, within the scope of their respective mandates, capacities and operational needs, to enhance their ability to ensure appropriate levels of ICT security and data protection, in accordance with Resolution 12, “Safeguarding humanitarian data”, adopted by the 2022 Council of Delegates, and *invites* States to support the Movement in these endeavours;
14. *recalls* that the processing of personal data is necessary for Movement components to perform their mandates, particularly under IHL, where applicable, and under the Statutes of the Movement, that such processing serves the furtherance of and is necessary on important grounds of public interest and the vital interests of people, and *urges* States and the Movement to cooperate to ensure that such personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of the Movement’s operations;
15. *encourages* States and Movement components to exchange knowledge and good practices, and build capacities in ICT security, data protection, international law and the protection of civilian populations and other protected persons and objects against the dangers arising from ICT activities, taking into account the different levels of resources available among States and Movement components.