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 cyber and information operations during armed conflict

DRAFT ZERO RESOLUTION

April 2024

EN
34IC/24/DRX.X
Original: English
Draft

Document prepared by the International Committee of the Red Cross in consultation with the IFRC

DRAFT ZERO RESOLUTION

Protecting civilians and other protected persons and objects against cyber and information operations 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, and information and communication realms, and can help save and improve lives, including in situations of armed conflict,

underlining the importance of information and communication technologies (ICTs) for the delivery of essential services – including medical and humanitarian services – to civilian populations, and for civilians to seek information about where to find safety, objects essential for their survival and to maintain family contact, including in situations of armed conflict,

noting that ICT capabilities are being used as means or methods of warfare in armed conflicts and their use in future conflicts is becoming more likely,

expressing concern that such use of ICT capabilities risks causing harm to the civilian population and other protected persons and objects in situations of armed conflict, in particular if cyber operations are directed against, or incidentally affect, ICTs that are part of or are used by civilian infrastructure and essential services,

acknowledging that States and National Red Cross and Red Crescent Societies with fewer ICT capacities may be particularly vulnerable to cyber operations,

expressing concern about the scale, speed and reach of disinformation and hate speech spread through ICTs, and the different risks of harm such information operations can cause to people affected by armed conflict, in particular people with specific needs, such as, among others, women, children and persons with disabilities,

noting that ICTs are used to enable or encourage civilians to conduct or support cyber or information operations in situations of armed conflict, and *expressing concern* that civilians may not be aware of the risks involved and 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 in situations of armed conflict,

recognizing that ICTs are essential for efficient and effective humanitarian operations, and *expressing* deep concern about the impact that cyber operations, including data breaches, and information operations designed to interfere with or undermine the work of humanitarian organizations risk having on these organizations and their personnel, affecting the delivery of humanitarian services to the people they serve,

recalling the legal and protective value of the distinctive emblems and signals, as applicable, and *welcoming* the research and consultation conducted by the International Committee of the Red Cross (ICRC), in collaboration with academic institutions and other components of the International Red

Cross and Red Crescent Movement (Movement), on the purpose, parameters and feasibility of a "digital emblem",[1]

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, and *welcoming* the commitments of the Movement on the protection of their humanitarian data,

recognizing 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, in particular in relation to international law,

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 inconsistent with the Charter of the United Nations, and *emphasizing* that recalling IHL by no means legitimizes or encourages conflict,

emphasizing that people, as well as medical and humanitarian organizations, also face harm caused by cyber and information operations in emergencies other than armed conflicts, *calling* on States to build on this resolution to take effective measures for their protection in line with applicable legal frameworks, and *asking* the Movement to take appropriate cyber 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 cyber and information operations;

2. *recalls* that IHL applies only to situations of armed conflict, including the established international legal principles of humanity, necessity, proportionality and distinction, and *clarifies* that even in situations of armed conflict, IHL applies only to conduct that has a nexus to that conflict;

3. *recognizes* the need for further study on how and when these principles apply to the use of ICTs, including cyber and information operations;

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 obligation to take constant care and all feasible precautions to avoid or minimize civilian harm, the prohibition of encouraging violations of IHL, and the prohibition of spreading terror among the civilian population serve to protect civilian populations and other protected persons and objects, including against the dangers arising from cyber and information operations;

5. *calls on* parties to armed conflicts to respect and protect medical personnel, units and transports exclusively engaged in medical duties in all circumstances, including with regard to cyber and information operations that would unduly interfere with their medical functions;

6. *further 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, including with regard to cyber and information operations that would unduly interfere with their humanitarian work;

[1] See ICRC, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions, 3 November 2022.

7. *demands* States and parties to armed conflicts implement and respect their international legal obligations applicable during armed conflict in ways that ensure the effective protection of the civilian population and other protected persons, as well as civilian objects;

8. *emphasizes* that, in situations of armed conflict, non-State actors must comply with the applicable domestic and international law that protects civilians and other protected persons and objects, and *calls on* States to disseminate knowledge of these rules as widely as possible in their respective countries, and to prosecute or suppress possible violations;

9. *encourages* all components of the Movement to consider the risk of harm caused by cyber and information operations for civilian population and other protected persons and objects, *urges* all components to improve their preparedness for and ability to respond to the risks of such operations, for instance by building capacity to detect such risks and conduct protection activities for affected populations, and *invites* States to support the Movement in these endeavours;

10. *encourages* States and Movement components to discuss directly with private technology companies the implications under domestic and international law of their providing ICT services in situations of armed conflict, and to engage with these companies to ensure their policies are consistent with the law applicable to situations of armed conflict, that their staff comply with their legal obligations, and that they take appropriate measures to protect their staff and civilian clients against possible harm;

11. *welcomes* the result of the ongoing research on, and testing of, a digital emblem, and *encourages* the ICRC, in consultation with States and Movement components, to continue its research and testing in order to further clarify the specific purpose and technical feasibility of a digital emblem, and to consult with States on the potential processes for the incorporation of the digital emblem into international law;

12. *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 cyber 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;

13. *recall*s 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 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;

14. *encourages* Movement components to exchange knowledge and best practices on cyber security, data protection, international law and the protection of civilian populations and other protected persons and objects against the dangers arising from cyber and information operations, taking into account the different levels of resources available to Movement components, and *invites* States to support such activities.