Power of humanity
34th International Conference
of the Red Cross and Red Crescent
28–31 October 2024, Geneva

Preventing and minimizing digital threats to people affected by armed conflict

DRAFT ELEMENTS OF RESOLUTION

November 2023

EN

Original: English

Document prepared by the International Committee of the Red Cross in consultation with the International Federation of the Red Cross and Red Crescent Societies

DRAFT ELEMENTS OF RESOLUTION

Preventing and minimizing digital threats to people affected by armed conflict

BACKGROUND

The draft elements of the proposed resolution on preventing and minimizing digital threats to people affected by armed conflict seek to provide an outline of the possible substance of individual paragraphs, without providing a definitive draft text. Each paragraph is followed by a rationale explaining why it would be useful to include such a paragraph in the resolution.

This document is being shared for consultation with the members of the International Conference of the Red Cross and Red Crescent in order to gather a first round of comments and feedback, and to gain an initial understanding of whether the proposed approach would be acceptable and garner consensus.

When providing comments and feedback on this document, please consider the following questions:

- Do you agree with the proposed elements for the preambular and operative paragraphs of the proposed resolution?
- Are there any elements that are missing or should be included in the resolution?

Detailed comments on the wording of the draft elements of this resolution are not expected at this stage. There will be an opportunity to comment on specific wording at a later stage, once the draft zero of the resolution is available.

INTRODUCTION

The availability and reliability of digital technology, infrastructure (including internet connectivity) and data is of significant importance and can save lives during emergencies, in particular armed conflicts. It enables people to survive by finding out where they can get, for instance, food, water and blankets and a safe place to stay, and allows them to contact and find family members they have lost contact with. It allows governments to provide essential services to populations and maintain civilian governance. The confidentiality, integrity and availability of digital technology and data is also essential for the functioning of medical services – both military and civilian – and an integral part of humanitarian operations, including those of the International Movement of the Red Cross and Red Crescent (Movement).

The digitalization of armed conflicts brings new threats for the life, safety and dignity of civilians, medical personnel, military personnel *hors de combat* and those who work to protect and assist them. While state and non-state actors have used digital means and methods of warfare to overcome their adversaries, such means and methods have also been used to disable critical civilian infrastructure and services, to incite violence against civilian populations, medical personnel and military personnel *hors de combat*, and to disrupt medical and humanitarian relief efforts or undermine trust in the latter. The malicious use of digital technologies is fuelling

conflicts, eroding trust and aggravating vulnerabilities. The growing use of artificial intelligence in such operations risks aggravating their scale and impact.

The ICRC, together with Movement partners, has been at the forefront of drawing attention to the threats posed to civilian populations, medical personnel and military personnel *hors de combat* by the digitalizing of military operations, and worked for the understanding and dissemination of knowledge of international humanitarian law applicable in armed conflicts, including with regard to cyber and information operations.

Moreover, the Movement has advanced the understanding of data protection in humanitarian operations (see "Handbook on Data Protection in Humanitarian Operations"), built international consensus around the importance of protecting data in the context of restoring family links (see 33rd International Conference, "Restoring family links while respecting privacy, including as it relates to personal data protection", and agreed on concrete measures by members of the Movement to safeguard humanitarian data (see 2022 Council of Delegates, "Safeguarding humanitarian data".

Governments have worked in United Nations forums on information and telecommunications in the context of international security and the protection of human rights in the digital space.

The proposed resolution, put forward in the unique humanitarian forum afforded by the International Conference of the Red Cross and Red Crescent, aims to draw attention to digital threats to civilian populations, medical personnel and military personnel *hors de combat*, and identify measures that states and members of the Movement could take to prevent or minimize such threats.

Preambular paragraphs (PP)

PP 1:
This preambular paragraph could underline the importance of the availability and integrity of digital technology, infrastructure (including internet connectivity) and data 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 indispensable to their survival and to maintain family contact, in particular during armed conflict.

Rationale:
Establishing a common understanding of the importance of digital technology, infrastructure and data for the lives, safety and dignity of people affected by armed conflict.

PP 2:
This preambular paragraph could recall that states are developing digital capabilities for military purposes and that these capabilities are being used in current armed conflicts and their use in future conflicts is becoming more likely, and express concern about such technologies being used to harm civilians and civilian populations, medical personnel, military personnel *hors de combat*, civilian objects and other protected persons and objects, or to cause such harm incidentally, and about the risk of such capabilities causing superfluous injury and unnecessary suffering.

Rationale:
Recognition of the military developments in this area and the potential human cost during armed conflict.

PP 3:
This preambular paragraph could express particular concern about the potential human cost caused by the direct and indirect effects of cyber operations that disrupt civilian infrastructure, services and data essential to human safety and dignity and the functioning of society.

Rationale:
Recognition of the potential human cost of cyber operations.

PP 4:
This preambular paragraph could express particular concern about the scale, speed and reach of digital information operations and the potential harm they can cause by inciting violence and hatred, raising tensions and undermining the availability and integrity of information that civilians need for their safety and survival in times of armed conflict.

Rationale:
Recognition of the potential human cost of information operations.

PP 5:
This preambular paragraph could express concern about civilians, in particular individuals, groups and companies, conducting cyber or information operations in relation to armed conflicts, and that such operations expose civilians to harm and undermine the principle of distinction.

Rationale:
Recognition of the risks involved when encouraging or tolerating civilians' involvement in cyber and information operations in relation to armed conflicts.

PP 6:
This preambular paragraph could express concern that the military use of civilian digital infrastructure, such as communication systems or clouds, risks turning such infrastructure into a military objective, and about the impact that attacks on such objects would have on civilians.

Rationale:
Recognition of the risk of using civilian objects for military purposes, which risks turning them into military objectives and thereby exposing them to harm.

PP 7:
This preambular paragraph could express concern about the risk that cyber operations, in particular indiscriminate ones, conducted in the context of an armed conflict risk incidentally affecting civilians beyond the territory of the parties to the conflict due to the global interconnectedness of cyberspace.

Rationale:
Recognition of the risk that cyber operations risk spreading and harming civilians across borders, especially if such attacks are indiscriminate.

PP 8:
This preambular paragraph could recall that tech companies provide a range of products, services and infrastructure on which civilian populations and governments rely, emphasize their responsibility to respect the rights of people affected by armed conflict, and underline the importance of including tech companies in discussions on the protection of civilians against digital threats during armed conflict.

Rationale:
Recognition of the particular role that tech companies play in the provision of digital products, services and infrastructure, including during armed conflict.

PP 9:
This preambular paragraph could recognize the importance of digital technology, infrastructure (including internet connectivity) and data for efficient and effective humanitarian operations,

and express deep concern about the impact that cyber operations, including data breaches, and information operations that target humanitarian organizations risk having on the people served by these organizations, the organizations themselves and their personnel.

Rationale:
Recognition of the importance of digital technologies, including data, to humanitarian organizations and the harm caused by targeting them.

PP 10:
This preambular paragraph could recall the legal and protective value of the distinctive emblems and signals, as applicable, for identifying medical units and transports, medical and religious personnel, as well as members of the International Red Cross and Red Crescent Movement, which, by virtue of their inclusion in the four Geneva Conventions and continuous practice for over 160 years, have become universally recognized symbols of impartial and neutral aid and protection to the victims of armed conflict and other emergencies, and it could welcome the research and consultation conducted by the ICRC, in collaboration with academic institutions and with other components of the Movement, on the feasibility of a "digital emblem",[1] i.e. a digital means of identifying the digital infrastructure and data of organizations and entities that are entitled to display the distinctive emblems recognized under international humanitarian law.

Rationale:
Recall the role of the distinctive emblems under international humanitarian law and welcome the ICRC's research and consultation on a possible "digital emblem".

PP 11:
This preambular paragraph could recall and reaffirm Resolution 4, "Restoring family links while respecting privacy, including as it relates to personal data protection", adopted by the 33rd International Conference, and emphasize that the issues addressed in that resolution are important for the protection of other humanitarian data.

Rationale:
Recalling and reaffirming the agreement reached at the 33rd International Conference on the protection of data in the Movement's work to restore family links.

PP 12:
This preambular paragraph could take note of Resolution 12, "Safeguarding humanitarian data", adopted by the 2022 Council of Delegates, and welcome the commitments of the Movement on the protection of humanitarian data.

Rationale:
Recognition of the work initiated in the Movement on the protection of humanitarian data.

PP 13:
This preambular paragraph could recall the conviction that nothing in international humanitarian law, including as applied to cyber or information operations, 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.

Rationale:
Recall the shared conviction among states as stated in the preamble of Additional Protocol I.

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

PP 14:
This preambular paragraph could emphasize that people, as well as medical and humanitarian organizations, also face digital threats in emergencies other than armed conflicts, call on states to build on this resolution to take effective measures for their protection in line with applicable legal frameworks, and ask the Movement to take appropriate cyber security and data protection measures at all times.

Rationale:
Recall the significance of digital threats outside armed conflicts and the need for states and Movement components to take protective measures outside armed conflicts.

Operative paragraphs (OP)

OP 1:
The operative paragraph could *emphasize* the shared commitment of all members of the International Conference to safeguard civilians, civilian objects and other persons and objects specifically protected during armed conflict against digital threats.

Rationale:
Expression of a shared humanitarian objective to protect civilians and civilian objects against digital threats during armed conflict.

OP 2:
The operative paragraph could *reaffirm* the fundamental importance of the obligations of all parties to armed conflicts under international humanitarian law, and other fields of international law, as applicable, in particular international human rights law, for the protection of civilians, civilian objects and other persons and objects specifically protected during armed conflict against cyber and information operations.

Rationale:
Reaffirmation of the existing legal framework applicable to cyber and information operations during armed conflict.

OP 3:
The operative paragraph could *call on* all states and all parties to armed conflicts to ensure that international humanitarian law is applied in ways that ensure adequate protection for civilians, medical personnel, military personnel *hors de combat*, civilian infrastructure and data, and other specifically protected persons and objects in increasingly digitalized societies; *demand respect* for the applicable rules; and *urge* all states and other actors that develop cyber or information capabilities to adopt the necessary legislative, administrative and practical measures domestically in order to implement their legal obligations.

Rationale:
Call on all states and all parties to armed conflicts to ensure adequate protection against digital threats and call for the implementation of applicable legal rules.

OP 4:
The operative paragraph could *call on* all states and parties to armed conflicts to respect, in particular, the cardinal principle of distinction under international humanitarian law to protect civilians against the danger of hostilities, including when conducting cyber and information operations; emphasize in particular that cyber capabilities that qualify as weapons, and are by nature indiscriminate, are prohibited; and underscore the prohibition of direct attacks against civilians and civilian objects, of acts or threats of violence the primary purpose of which is to spread terror among the civilian population, of attacks that are indiscriminate and disproportionate, of attacking, destroying, removing or rendering useless objects that are

indispensable to the survival of the population, and of perfidy as well as of the improper use of specifically protected emblems, signals, flags, uniforms and insignia, including when using digital means and methods of warfare; and *recall* the obligations to take constant care to spare the civilian population and civilian objects and to take all feasible precautions to avoid or at least minimize incidental civilian harm and to protect the civilian population and civilian objects under their control against the effects of attacks, including when using digital means and methods of warfare.

Rationale:
Reaffirmation of some of the basic rules of IHL protecting civilians against digital threats during armed conflicts.

***OP 5**:*
This operative paragraph could *also call on* states and parties to armed conflicts to respect the obligation under international humanitarian law to respect and protect medical personnel, units and transports in all circumstances, including against cyber and information operations.

Rationale:
Reaffirmation of the specific international legal protection of medical units, transports and personnel against digital threats during armed conflict.

OP 6:
The operative paragraph could *further call on* states and parties to armed conflicts to respect the obligations under international humanitarian law to allow and facilitate impartial humanitarian activities during armed conflict, including those carried out by digital means, and to respect and protect humanitarian activities and personnel, including against cyber and information operations.

Rationale:
Reaffirmation of the specific international legal protection of impartial humanitarian organizations against digital threats during armed conflict.

OP 7:
The operative paragraph could *recall* that when parties to an armed conflict encourage civilian involvement in an armed conflict, including though digital means, civilians risk losing their legal protection against attack, or being perceived to have lost their protection, and *call on* parties to bear this in mind and to take all feasible precautions to avoid exposing civilians to harm.

Rationale:
Recognition of the risks entailed when encouraging civilians to take part in hostilities, and a call to take all feasible precautions to protect civilians.

OP 8:
The operative paragraph could *emphasize* that non-state actors, including civilians and non-state armed groups, who conduct cyber operations in relation to an armed conflict must, regardless of their status, comply with international humanitarian law, *reaffirm* states' commitment to take measures to ensure that non-state actors operating under a state's instructions, direction or control, or from its territory, do not conduct operations in violation of international humanitarian law, and supress possible violations thereof, and *encourage* the ICRC and National Red Cross and Red Crescent Societies to renew their efforts to disseminate knowledge of international humanitarian law.

Rationale:
Reaffirmation of states' primary role in ensuring respect for international humanitarian law by non-state actors, and recognition of the Movement's statutory role in raising awareness of IHL.

OP 9:
This operative paragraph could *recall* that tech companies that operate in, or provide services in relation to, contexts affected by armed conflicts should understand and consider the implications of their operations under international humanitarian law, ensure that their staff comply with relevant obligations and take appropriate measures to protect against possible harm their staff and any civilians that rely on their products and services.

Rationale:
Call on tech companies to invest in understanding the implications of their operations during armed conflict and to take steps to protect civilian populations.

OP 10:
The operative paragraph could *encourage* states to segment, i.e. physically or technically separate, to the extent feasible, digital infrastructure used for military purposes from civilian infrastructure, recognizing that the use of civilian infrastructure for military purposes risks turning it into a military objective, which could have a harmful impact on civilians who are also using that infrastructure.

Rationale:
Encouragement of states to segment, to the extent feasible, digital infrastructure used for military purposes from infrastructure used for civilian purposes.

OP 11:
This operative paragraph could *encourage* all members of the Movement, as part of their work, to consider digital threats and the related harm, *urge* all members to improve their preparedness for and ability to respond to digital threats against civilians, for instance by building capacity to detect threats and conduct protection activities for civilian populations, and *invite* states to support the Movement in these endeavours.

Rationale:
Encourage the Movement to strengthen its capacity to respond to digital threats and invite states to support the necessary investment and capacity building.

OP 12:
The operative paragraph could *welcome* the result of the ongoing research on, and testing of, a digital emblem, and *encourage* the ICRC, in consultation with states and Movement components, to propose a technical, comprehensive and lasting solution, and put forward options for states for incorporating it into international humanitarian law.

Rationale:
Invite the ICRC to continue work on a digital emblem closely with states and the Movement.

OP 13:
This operative paragraph could *commit* 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; to apply best practices in data governance for all humanitarian data; to implement relevant standards and good practices in the processing of personal data, taking into consideration the Handbook on Data Protection in Humanitarian Action; and to comply with applicable law and personal data protection frameworks, and *express* states' support for these measures.

Rationale:
Commitment by the Movement to take appropriate cyber security and data protection measures to protect the populations they serve.

OP 14:
This operative paragraph could *recall* that the processing of personal data is necessary for Movement components to perform their mandates, particularly under international humanitarian law, 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 could *urge* 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, and in accordance with Article 2, including paragraph 5 thereof, of the Statutes 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.

Rationale:
Recollection of the importance of data processing in the humanitarian work of the Movement and for states' cooperation in fulfilling the Movement members' respective mandates.

OP 15:
This operative paragraph could *invite* the ICRC to continue assessing digital threats during armed conflicts and the protection of civilians against them, including under international humanitarian law, and report back to the 35th International Conference on this subject.

Rationale:
Invite the ICRC to report back to the next International Conference on the subject of this resolution.