ICRC

PROTECTION OF HUMANITARIAN PERSONNEL AND OBJECTS DURING ARMED CONFLICT

Parties to armed conflicts must allow and facilitate impartial humanitarian activities during armed conflict, and respect and protect humanitarian personnel and objects used for humanitarian operations, in accordance with international humanitarian law, including with regard to information and communications technology activities.

Humanitarian organizations increasingly rely on digital technologies to assist and protect people affected by armed conflicts. **As the world faces staggering humanitarian needs, humanitarian operations risk disruption** by rapidly evolving ICT threats. The UN Security Council has expressed 'concern about the increase in malicious information and communication technologies activities, including data breaches, information operations, that target humanitarian organizations, disrupt their relief operations, undermine trust in humanitarian organizations and United Nations activities, and threaten the safety and security of their personnel, premises and assets, and ultimately their access and ability to carry out humanitarian activities'.[1]

As the world faces staggering humanitarian needs, humanitarian operations risk disruption by rapidly evolving ICT threats.

In situations of armed conflict, international humanitarian law (IHL) imposes limits on the conduct of cyber operations (when does IHL apply? ↗), including in relation to the protection of humanitarian personnel and objects used for humanitarian operations.

Under IHL, humanitarian personnel and objects used for humanitarian operations are civilian, meaning they must not be attacked, in accordance with the principle of distinction ↗. All feasible precautions must be taken to avoid, and in any event to minimize, incidental loss of civilian life and injury or damage to humanitarian personnel and objects.[2]

The specific obligations of IHL with respect to humanitarian operations are found largely under two rules, both of which must be complied with including with regard to ICT activities.[3] First, parties to the conflict must allow and facilitate rapid and unimpeded passage of humanitarian operations for civilians in need, which are impartial in character and conducted without any adverse distinction, subject to their right of control. And two, parties to armed conflict must respect and protect humanitarian personnel and objects used for humanitarian operations. These obligations derive from specific treaty rules in the Geneva Conventions and their Additional Protocols.[4]

1 UN, Security Council, ***Resolution 2730*** (2024), 24 May 2024, preamble.
2 Additional Protocol I (1986), Article 57.
3 34th International Conference of the Red Cross and Red Crescent, ***Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict***, Resolution 34IC/24/R2, 2024, OP 7.
4 Fourth Geneva Convention (1949), Article 23; Additional Protocol I (1977), Articles 70, 71; Additional Protocol II (1977), Article 18.

Today, they are also part of customary international law and apply both in international and non-international armed conflicts,[5] binding state and non-state parties to armed conflict.[6] Accordingly, the 2024 the International Conference of the Red Cross and Red Crescent called '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'.[7]

The **obligation to allow and facilitate rapid and unimpeded passage of humanitarian operations for civilians in need** requires a party to a conflict to 'do all it can to facilitate the passage of relief consignments', without being expected to do the impossible.[8] With regard to ICT activities, this includes reducing bureaucracy for humanitarian organizations to import and use ICTs, and facilitate Internet access, including through satellite connections, as needed for efficient and safe humanitarian operations.

Linked to the obligation to allow and facilitate humanitarian activities is the obligation to **respect and protect humanitarian personnel and objects used for humanitarian operations**. This obligation prohibits parties to the conflict from attacking any object used for humanitarian operations, including ICT objects (such as phones, computers, servers, among others). Intentionally directing attacks against personnel, installations, material, units or vehicles involved in a humanitarian assistance mission, as long as they are entitled to the protection given to civilians or civilian objects under the international law of armed conflict, constitutes a war crime.[9]

The obligation to respect objects used for humanitarian operations is broader than only sparing them against cyber operations that amount to attacks as defined in IHL. Similar to the obligation to respect and protect medical personnel and facilities, IHL rules on the protection of humanitarian personnel and objects must also be understood as prohibiting "other forms of harmful conduct outside the conduct of hostilities" against humanitarians or undue interference with their work.[10] This prohibition includes, for instance, the intentional disruption of the ability of humanitarian personnel to communicate for operational purposes.

Parties to the conflict must protect humanitarian operations and personnel from harm caused through ICT activities.

Likewise, allowing and facilitating humanitarian operations, and respecting objects used for such operations, requires not to damage, delete, or manipulate **data processed for humanitarian purposes**. In addition, a party that agrees to humanitarian services and acts in good faith should respect the confidentiality of data processed for humanitarian purposes, and must not access any confidential data that is explicitly protected under IHL, or essential to carry out the humanitarian functions assigned to humanitarian organization under IHL treaties.[11]

The **obligation to protect** requires all parties to the conflict to take positive steps to protect humanitarian personnel and objects from harm, including harm caused through ICT activities.[12] Accordingly, if a party to an armed conflict learns of the existence of a serious cyber threat to a humanitarian operation – or an ongoing harmful cyber operation – and if it is in its power to address that situation, it is obliged to take feasible steps to protect the

5 ICRC, Study on Customary International Humanitarian Law: Volume I, Rules 31, 32, 55.

6 This includes individual hackers of hacker groups. See ICRC, ***Eight rules for "civilian hackers" during war, and four obligations for states to restrain them***, 2023.

7 International Conference of the Red Cross and Red Crescent, Resolution 34IC/24/R2, October 2024, para. 7.

8 ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 1977, para. 2829 on article 70.

9 See Rome Statute of the International Criminal Court (1998), Articles 8(2)(b)(iii), 8(2)(b)(xxiv), and 8(2)(e)(iii).

10 See ICRC Commentary on the First Geneva Convention, para 1799 on article 19. As the Tallinn Manual states, efforts to provide humanitarian assistance are protected against cyber operations "even if they do not rise to the level of an 'attack'". also M. N. Schmitt and L. Vihul (eds), ***Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations***, Cambridge University Press, 2017, para. 4 of the commentary on Rule 80 (Tallinn Manual 2.0).

11 For example, Third Geneva Convention (1949), Article 126 and Fourth Geneva Convention (1949), Article 143, grant the ICRC the right to interview the prisoners of war and civilian internees without witnesses. Any records from such confidential interviews must be protected against any unauthorized access, including by ICT activities. See also International Conference of the Red Cross and Red Crescent, Resolution 33IC/19/R4, December 2019, paras 10-11.

12 See similarly ICRC Commentary on the First Geneva Convention, para. 1808 on article 19; Tallinn Manual 2.0, para 6 of the commentary on Rule 131.

humanitarian organization. This includes protection against harmful cyber operations conducted by 'hacktivists' or other non-state actors.

The obligation to allow and facilitate the rapid and unimpeded passage of humanitarian operations for civilians in need is **subject to a party's right of control**, and belligerents may prescribe the technical arrangements, including search, under which such passage is permitted.[13] In the ICT context, this may mean verifying that communication devices or platforms are only used for humanitarian purposes, or that digital cash assistance is not diverted.

In the physical world, humanitarian operations conducted by a red cross or red crescent organizations are often identified by a **distinctive emblem**, such as a red cross, red crescent, or red crystal, and may use distinctive radio, light or electronic signals, to signal their specific legal protection. The ICRC is currently exploring how a 'digital emblem' could be developed to the same effect for digital assets.[14] Similar technologies may also be used in the future to identify other digital assets specifically protected under IHL, including those associated with cultural property, dangerous forces, and civil defence.

13 Additional Protocol I (1977), Article 70(3); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 55.
14 ICRC, *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions*, 2022.

ICRC
International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01

02.2025