

PROTECTION OF MEDICAL PERSONNEL, UNITS AND TRANSPORTS DURING ARMED CONFLICT

Parties to armed conflicts must respect and protect medical personnel, units and transports in all circumstances, in accordance with international humanitarian law, including with regard to information and communications technology activities.

Recent years have seen a significant number of cyber operations against hospitals and other medical facilities. According to information and communications technologies (ICT) experts, the healthcare sector is particularly vulnerable to cyber harm.¹ This is due to its growing digitalization, which increases the attack surface, both in ordinary computers used by hospitals and in specialized medical devices such as MRI scanners or pacemakers.² Accordingly, States have underscored the vulnerability of the healthcare sector to malicious ICT activities, and expressed concern about them.³

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 medical personnel, units and transports. The protection of the medical services is one of the oldest IHL rules,⁴ recognizing that in times of armed conflict combatants and civilians that suffer injuries or diseases must be cared for.

The relevant rules of IHL are well-established: **parties to armed conflict must respect and protect medical facilities and medical personnel in all circumstances**, including when carrying out cyber operations. These obligations derive from specific treaty rules in the Geneva Conventions and their Additional Protocols.⁵ Today, they are also part of customary international law and apply equally in international and non-international armed conflicts,⁶ binding States and non-state parties to armed conflict.⁷ Accordingly, the 2024 International Conference of the Red Cross and Red Crescent called 'on parties to armed conflicts to respect and protect medical personnel, units and

The healthcare sector is vulnerable to malicious ICT activities, and especially so during armed conflicts.

¹ ICRC, *The Potential Human Cost of Cyber Operations*, 2019, p. 6.

² *Ibid.* p. 20.

³ UN, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, 2021 (GGE report), para. 10; UN, *progress Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025*, 2024, para. 14.

⁴ Convention for the Amelioration of the Condition of the Wounded in Armies in the Field (1864), article 1.

⁵ See e.g. Geneva Convention I (1949), Article 19; Geneva Convention II (1949), Article 12; Geneva Convention IV (1949), Article 18; Additional Protocol I (1977), Article 12; Additional Protocol II (1977), Article 11.

⁶ ICRC, *Study on Customary International Humanitarian Law*, 2005, rules 25, 28, and 29.

⁷ 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.

transports in accordance with their international legal obligations, including with regard to ICT activities'.⁸

The **obligation to respect** requires parties to the conflict to refrain from behaviour that would interfere with their work, which includes the functioning of all ICT components of medical facilities and the work of medical personnel.⁹ First and foremost, this means refraining from directing attacks against such facilities. Intentionally directing attacks against medical units and transports constitutes a war crime.¹⁰



The obligation to respect medical facilities is, however, broader than only sparing medical facilities from cyber operations that amount to attacks as defined in IHL. It is also prohibited to unduly interfere with the functioning of medical services in any other way. It is therefore immaterial whether the interference leads to death or injury or merely slows down the functioning of a medical facility.

The purpose of the obligation to respect medical facilities is to allow them to continue to treat the wounded and sick in their care. Interference with their operations, including the intentional disruption of medical units' ability to communicate for medical purposes, violates the duty to respect medical facilities.¹¹ Likewise, a cyber operation that, for instance, renders the hospital's computer systems inoperable, disables its IT infrastructure, or deletes, tamper with or encrypts patient or other medical data interferes with the hospital's functioning and is prohibited by IHL.

Parties to the conflict must protect medical facilities and personnel from harm caused through digital means.

The **obligation to protect** requires all parties to the conflict to take positive steps to protect medical facilities and personnel from harm, including from 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 medical facility – 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 medical facility. This includes protection against harmful cyber operations conducted by non-state actors in the context of and associated with an armed conflict.

Medical personnel, units and transports only lose their protection under IHL, including from cyber operations, if they commit, outside their humanitarian function, acts harmful to the enemy; the protection only ceases, however, after a due warning has been given and is unheeded.¹³ This would be the case if medical facilities are used to interfere directly or indirectly in military operations, and thereby cause harm to the enemy.¹⁴ In the cyber context, conduct that could qualify includes using the computer systems of medical facilities to launch offensive cyber operations against the enemy's networks.

The specific protection of medical facilities may only cease after a due warning has been issued and, where appropriate, a reasonable time limit has been set.¹⁵ In addition, any cyber operation taken in response to such acts harmful to the enemy would still have to comply with all other applicable rules of IHL, in particular the principles of [distinction](#) , [proportionality](#) , and precautions.

In the physical world, medical objects and personnel are commonly identified by a **distinctive emblem**, such as a

⁸ International Conference of the Red Cross and Red Crescent, Resolution 34IC/24/R2, October 2024, para. 6.

⁹ ICRC, *Commentary on the First Geneva Convention*, 2016 (ICRC GC I Commentary), para. 1799 on article 19.

¹⁰ See Rome Statute of the International Criminal Court (1998), Articles 8(2)(b)(ix), 8(2)(b)(xxiv) and 8(2)(e)(ii). See also Additional Protocol I (1977), Article 85(2).

¹¹ ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, 1987 (ICRC AP Commentary), para. 517. See also ICRC GC I Commentary, para. 1799 and 1804; *Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector* (21 May 2020), point 5; Tallinn Manual 2.0, para 5 of the commentary on Rule 131.

¹² ICRC GC I Commentary, para. 1808; Tallinn Manual 2.0, para 6 of the commentary on Rule 131.

¹³ Geneva Convention I (1949), Article 21; Geneva Convention II (1949), Article 34; Geneva Convention IV (1949), Article 19; Additional Protocol I (1977), Article 13; Additional Protocol II (1977), Article 11; ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 25, 28, and 29.

¹⁴ ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, p. 43.

¹⁵ Geneva Convention I (1949), Article 21; Geneva Convention II (1949), Article 34; Geneva Convention IV (1949), Article 19; Additional Protocol I (1977), Article 13; Additional Protocol II (1977), Article 11.

red cross, red crescent, red crystal or red lion and sun, and may use distinctive radio, light or electronic signals, to signal their specific legal protection.¹⁶ The ICRC is currently examining how a ‘digital emblem’ could be developed to the same effect.¹⁷ 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.

-
- ¹⁶ Geneva convention I (1949), Articles 38–44; Additional Protocol I (1977), Article 18; Annex I to Protocol Additional I (1977): Regulations concerning identification, as amended on 30 November 1993, Article 6–9.
- ¹⁷ ICRC, *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions*, 2022.