

THE PRINCIPLES OF HUMANITY AND NECESSITY

The fundamental principles of humanity and military necessity underlie and inform the entire normative framework of international humanitarian law (IHL). All rules of IHL reflect a careful balance between these two principles, which in turn inform the interpretation of these rules. The two principles also impose limits beyond specific rules, including in the information and communications technology environment.

The **balance between humanitarian considerations and military necessity is a hallmark of IHL**. In the cyber context, the UN Group of Governmental Experts has noted the principles of humanity and necessity as ‘established international legal principles’ and identified the ‘need for further study on how and when’ they apply to the use of information and communication technologies by States.¹

The balance between humanity and necessity underlies and informs the entire normative framework of IHL. It shapes the context in which its rules and other principles (such as [distinction](#) ², [proportionality](#) ², and precautions) must be interpreted. Considerations of military necessity and humanity neither derogate from nor override the specific rules of IHL, but constitute guiding principles for the interpretation of the rights and duties of parties to armed conflicts within the parameters set by these rules.²

One of the great strengths of IHL is – as pointed out by the International Court of Justice – that it is designed in such ways that it applies ‘to all forms of warfare and to all kinds of weapons’, including ‘those of the future’.³ The same rules and principles – including the fundamental principles of humanity and military necessity – apply to all military operations, be they kinetic or cyber in nature, and they must be respected at all times.⁴

Military necessity and humanity constitute guiding principles for the interpretation of all rules of IHL.

There are two general approaches to the **legal effect of the principles** of humanity and military necessity. The narrower view considers that while the two principles inform the entire body of IHL, they do not create obligations above and beyond specific rules of IHL. The broader view considers that these principles impose limits beyond specific IHL rules: even if a cyber operation during an armed conflict is not prohibited by a specific rule of IHL, to be lawful it must nonetheless comply with the principles of military necessity and humanity. The ICRC takes this latter view.⁵

The **principle of military necessity** requires that a party to an armed conflict may only resort to those means and

¹ UN, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, July 2021, para. 71(f); see also UN, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025*, August 2022, para. 15(b)(ii).

² ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 2009 (ICRC DPH Guidance), pp. 78–79.

³ ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996, para. 86.

⁴ ICRC, *International humanitarian law and cyber operations during armed conflicts: Position paper*, 2019, p. 4.


⁵ See ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, 1987 (ICRC AP Commentary), para. 1395; ICRC DPH Guidance, pp. 77–82; ICRC, *Commentary on the Third Geneva Convention*, 2020, para. 497.

methods that are necessary to achieve the legitimate purpose of a conflict, i.e. ‘to weaken the military forces of the enemy’.⁶ It does not, however, permit the taking of measures that would otherwise be prohibited under IHL,⁷ and a rule of IHL cannot be derogated from by invoking military necessity unless this possibility is expressly provided for by the rule in question.⁸

For example, cyber operations that do not constitute attacks under IHL but that would nonetheless seize or destroy enemy property (such as freezing access to data stored in the cyber infrastructure controlled by the other party to the conflict) may be justified on the grounds that such seizure or destruction would be ‘imperatively demanded by the necessities of war’.⁹ By contrast, IHL mandates that medical facilities be respected and protected at all times,¹⁰ which precludes the reliance on military necessity to justify a cyber operation against a hospital during an armed conflict – although such facilities may lose their protection under IHL, including from cyber operations, under very narrow and well-defined circumstances.¹¹

The **principle of humanity** imposes certain limits on the means and methods of warfare, and requires that those who have fallen into enemy hands be treated humanely at all times.¹² It seeks to limit suffering, injury, and destruction during armed conflict; its purpose is to protect life and health and to ensure respect for the human being. This principle precludes the assumption that anything that is not explicitly prohibited by specific IHL rules is therefore permitted.¹³

For instance, using disinformation to mislead the enemy is not as such prohibited, as long as it does not infringe any specific rule of IHL and is not perfidious.¹⁴ Conversely, spreading false information designed to cause panic among the civilian population in times of armed conflict would conflict with the principle of humanity. This is because such actions – even if not covered by a particular rule of IHL¹⁵ – would be reasonably expected to lead to significant harm to civilians, which would be contrary to the demands of humanity.

The **conjunction of both principles** is particularly important in cases where the interpretation of the existing law to cyber operations is unsettled. For example, a few States disagree with the view – held by several other States and the ICRC – that a cyber operation designed or expected to result in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL (see [distinction](#) ). However, if such an operation was not actually necessary for the accomplishment of a legitimate military purpose in a particular situation, it would be inconsistent with the principles of military necessity and humanity regardless of whether it was considered as an attack. Accordingly, even parties to armed conflicts that would not regard it as an attack must at least in such circumstances refrain from launching the operation.¹⁶

*The principles of humanity
and military necessity
are particularly important
in cases where the law
is unsettled.*

⁶ St. Petersburg Declaration (1868), preamble.

⁷ United States, Military Tribunal at Nuremberg, *Hostages case*, Judgment, 1948, pp. 66–67 (‘[m]ilitary necessity or expediency do not justify a violation of positive rules’).

⁸ ICRC AP Commentary, para. 1389.

⁹ Hague Regulations (1907), Article 23(g).

¹⁰ See e.g. First Geneva Convention (1949), Article 19; Second Geneva Convention (1949), Article 12; Fourth Geneva Convention (1949), Article 18; Additional Protocol I (1977), Article 12; Additional Protocol II (1977), Article 11; ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 25, 28, 29.

¹¹ ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015, p. 32.

¹² Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction*, ICRC, 2022, p. 19.

¹³ ICRC AP Commentary, para. 55.

¹⁴ Additional Protocol I (1977), Article 38(2).

¹⁵ The following rules may prohibit such an operation, depending on the circumstances: Fourth Geneva Convention (1949), Article 33; Additional Protocol I (1977), Article 51(2); Additional Protocol II (1977), Article 13(2); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 2.

¹⁶ See e.g. United States, Law of War Manual, 2016, p. 1022, para. 16.5.2.