

THE PRINCIPLE OF PROPORTIONALITY

In the use of information and communications technologies, the principle of proportionality prohibits parties to armed conflicts from launching a cyber attack against a military objective which may be expected to cause incidental civilian harm that would be excessive in relation to the concrete and direct military advantage anticipated.

Applying the **principle of proportionality** is critically important for protecting civilians and critical infrastructure in situations of armed conflict, especially because civilian and military networks are highly interconnected in the information and communications technology (ICT) environment and incidental civilian harm is to be expected in most cases.

The principle of proportionality is codified in Article 51(5)(b) of the 1977 Additional Protocol I, which reflects customary international law.¹ It prohibits attacks ‘which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated’.

The UN Group of Governmental Experts has noted the principle of proportionality as one of the ‘established international legal principles’ in the context of how international law applies to the use of ICTs by States and identified the ‘need for further study on how and when’ it applies.²

The principle of proportionality is a corollary of the [principle of distinction](#) and it recognizes that, in the conduct of hostilities, causing incidental harm to civilians and civilian objects is often unavoidable.³ However, it places a limit on the extent of incidental civilian harm that is permissible whenever military objectives are attacked, by spelling out how the [principles of humanity and necessity](#) must be balanced in such situations.

The principle of proportionality is further reinforced by certain rules flowing from the principle of precautions in attack, in particular the obligation to do everything feasible to assess whether an attack may be expected to be disproportionate and to cancel or suspend an attack if it becomes apparent that it may be expected to have disproportionate effects.⁴ Overall, an attack against a military objective can be lawful only if the principles of proportionality and precautions are respected, meaning that the incidental civilian harm must not be excessive, and the attacker must have taken all feasible precautions to avoid this harm or at least reduce it.

The principle of proportionality limits the extent of permissible incidental civilian harm caused by cyber attacks.

¹ ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 14.

² 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).

³ ICRC, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under IHL*, 2018 (ICRC Proportionality Report), p. 8


⁴ Additional Protocol I (1977), Articles 57(2)(a)(iii) and 57(2)(b); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 18 and 19.

The notion of ‘**incidental civilian harm**’ is an umbrella term that covers three types of harm specifically listed in Article 51(5)(b) of Protocol I, namely loss of civilian life, injury to civilians, and damage to civilian objects. The type and extent of civilian harm caused by cyber operations may significantly differ from that caused by kinetic operations. Among other differences, a cyber operation could incidentally disable civilian objects without physically damaging them; but the effects may be more widespread due to the interconnectedness of cyberspace.⁵

The assessment of incidental civilian harm includes harm due to the foreseeable direct and indirect effects of cyber operations.⁶ Direct harm in this context refers to consequences that are directly and immediately caused by a cyber attack, such as damage to the targeted systems. Indirect harm – also referred to as ‘reverberating effects’ – covers all other consequences that may foreseeably result from the cyber attack in question.⁷ In the ICT context, they may include effects on the infrastructure controlled by the targeted system or on other objects or persons affected by the malfunction or destruction of those systems.⁸

The relevant civilian harm that must be considered in the application of this rule includes that occasioned in transit – such as damage to the cyber infrastructure through which a cyber operation may be routed – as well as that caused by the effect of the cyber attack on the targeted system.⁹ The consequences for civilians of impairing the civilian use of objects employed simultaneously for civilian and military purposes (such as elements of the power grid, depending on the circumstances) must also be considered.¹⁰

What is foreseeable at the moment of a cyber attack is to be assessed from the perspective of the ‘reasonable commander’, namely a person trained and experienced in the military art, making use in good faith of information from all sources reasonably available to them in the circumstances. It is generally agreed that in the context of military cyber operations, such sources should include appropriate technical expert advice.¹¹

The incidental harm to be taken into consideration raises the question of whether incidental loss of functionality of civilian computers, systems or networks needs to be considered for the application of the principle of proportionality. In the ICRC’s view, any type of harm relevant to the protection of civilian objects against direct attack must be taken into consideration, including when such objects are disabled¹² (see also [principle of distinction](#) )

Cyber operations pose new challenges for the assessment and avoidance of incidental civilian harm.

The expected incidental civilian harm must be compared with the anticipated ‘**concrete and direct military advantage**’. Because of the requirement that the advantage must be ‘military’ in character, advantages which are solely political, psychological, economic, financial, social or moral must be excluded from the equation.¹³ It is generally agreed that neither disrupting government propaganda nor undermining the morale of the population offers a concrete and direct military advantage.¹⁴

The qualifier ‘concrete’ means that speculative, hypothetical, or general benefits may not be taken into consideration. Therefore, those who plan and decide upon a cyber attack must be sufficiently certain that the attack will result in a real and quantifiable advantage.¹⁵

The term ‘direct’ requires a causal relation between the cyber attack and the anticipated military advantage¹⁶

⁵ ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, 2021, p. 19.

⁶ ICRC, *International humanitarian law and cyber operations during armed conflicts: Position paper*, 2019 (ICRC position paper), p. 9.

⁷ ICRC Proportionality Report, p. 43.

⁸ See e.g. France, *International Law Applied to Operations in Cyberspace*, 2019, p. 16.

⁹ M. N. Schmitt and L. Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017 (Tallinn Manual 2.0), commentary on Rule 113, para. 3.

¹⁰ United States, *Law of War Manual*, 2016, p. 1021, para. 16.5.1.1; ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2019, p. 19.

¹¹ ICRC Proportionality Report, pp. 49 and 59.

¹² ICRC position paper, pp. 7–8.

¹³ *Manual on International Law Applicable to Air & Missile Warfare*, 2009, commentary on Rule 1(w), para. 4.

¹⁴ ICRC Proportionality Report, p. 12.

¹⁵ Tallinn Manual 2.0, commentary on Rule 113, para. 9.

¹⁶ ICRC Proportionality Report, p. 18.

such that there is no ‘intervening condition or agency’.¹⁷ Accordingly, an advantage that is remote in nature or that would only appear in the long term should be disregarded.¹⁸

If a cyber operation is executed in a concerted manner with other types of military action, such as kinetic attacks directed against the same military objective, the military advantage must be considered with regard to the attack as a whole and not only on the basis of each separate action.¹⁹ However, the attack as a whole still constitutes a finite operation with defined limits and must not be confused with the entire war effort.²⁰

The principle of proportionality **must be respected by the parties to an armed conflict in all circumstances**, even if alternative, more discriminate weapons or tactics – whether cyber or kinetic – are not available to them.²¹ In applying this principle, the parties to armed conflicts must be guided by the ‘basic obligation to spare civilians and civilian objects as much as possible’.²²

Some States have published their basic **procedures for assessing compliance** with the principle of proportionality (also known as ‘collateral damage estimation methodologies’). However, the details on how these are conducted in practice tend not to be released, which is particularly the case with military cyber capabilities. Accordingly, States that decide to resort to cyber operations during armed conflicts should use the existing processes developed for the purposes of kinetic operations as a general frame of reference and adapt them to account for the specific nature of, and the challenges posed by, cyber operations.²³

¹⁷ M. Bothe et al., *New Rules for Victims of Armed Conflicts*, Martinus Nijhoff, 1982 (Bothe et al.), p. 407.

¹⁸ ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, 1987 (ICRC AP Commentary), para. 2209; Bothe et al., p. 407.

¹⁹ ICRC AP Commentary, para. 2218; Tallinn Manual 2.0, commentary on Rule 113, para. 10.

²⁰ See International Law Association, ‘The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare’, *International Law Studies*, Vol. 93, 2017, pp. 343 and 364.

²¹ ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015, p. 50.

²² ICTY, *Galić Trial Judgment*, 2003, para. 58; see also Additional Protocol I (1977), Article 57(1), and ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 15.

²³ ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, 2021, p. 24; see also France, *International Law Applied to Operations in Cyberspace*, 2019, p. 13.