ICRC

THE PRINCIPLE OF DISTINCTION

In the use of information and communications technologies, the principle of distinction requires that parties to an armed conflict at all times distinguish between civilians and combatants and between civilian objects and military objectives. Cyber attacks may only be directed against combatants or military objectives. Cyber attacks must not be directed against civilians or civilian objects. Indiscriminate cyber attacks are prohibited.

The principle of distinction is one of the oldest principles and a cornerstone of international humanitarian law (IHL). The International Court of Justice considers it a 'cardinal' and 'intransgressible' principle that forms part of the 'fabric' of IHL.[1] It applies only in the context of an armed conflict and prohibits directing attacks against civilians and civilian objects.[2] The UN Group of Governmental Experts has noted the principle of distinction as one of the 'established international legal principles' in the context of how international law applies to the use of information and communications technologies (ICTs) by States and identified the 'need for further study on how and when' it applies.[3]

When using ICTs in the context of armed conflicts, **the obligation to direct cyber attacks only against military objectives and not against civilian objects** is particularly important. In IHL, civilian objects are defined as all objects that are not military objectives.[4] Military objectives are limited to 'objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.[5] This means that civilian infrastructure (including water and electricity plants, private property, or civilian government ICT equipment and infrastructure) or any other civilian object must not be attacked. Under IHL, the qualification of civilian infrastructure as 'critical infrastructure' has no legal importance.

The principle of distinction is a cardinal principle that forms part of the fabric of IHL.

In the ICT environment, civilians and the military generally use the same Internet infrastructure (such as cables, satellites, routers or nodes) and might rely on the same digital communication, storage and other services. This is often referred to as 'dual use' of an object. The use of civilian ICT infrastructure for military purposes may turn such objects into military objectives. This can, however, only be the case if the two above-mentioned cumulative conditions are met: (1) the use of such object or infrastructure must make an effective contribution to military action and (2) its destruction, capture or neutralization must offer a definite military advantage. For example, even though a civilian undersea fibre cable may be used for military purposes, it would

1 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996, paras 78–79.
2 Additional Protocol I (1977), Articles 48, 51, and 52; ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 1 and 7.
3 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).
4 Additional Protocol I (1977), Article 52(1); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 9.
5 Additional Protocol I (1977), Article 52(2); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 8.

be questionable whether its destruction would offer a definite military advantage because the data passing through such cable may simply reroute and find its addressee nonetheless. Moreover, even if civilian infrastructure qualifies as a military objective, any attack against it would need to comply with all other IHL rules, in particular the principles of proportionality and precaution. It would be a matter of serious concern if the military use of cyberspace led to the conclusion that many objects that form part thereof would no longer be protected against attack. This could lead to large-scale disruption of the ever-increasingly important civilian usage of ICT services.[6]

The principle of distinction prohibits indiscriminate attacks, including when using cyber means or methods of warfare. Indiscriminate attacks are types of attacks that are of a nature to strike military objectives and civilian objects without distinction.[7] This includes cyber attacks that are not directed at a specific military objective, such as a cyber operation aimed at wiping the computers of all government agencies of an adversary, consisting of civilian and military agencies; cyber attacks which employ means or methods of warfare that cannot be directed at a specific military objective, such as a malware that exploits a vulnerability found in civilian and military systems, self-propagates and is released into an open network; and cyber attacks which employ means or methods of warfare the effects of which cannot be limited as required by IHL, such as a cyber operation that is targeted at a military objective but, once released, will spread without limits and may be expected to cause disproportionate harm to civilians.

States have taken different views on what types of cyber operations qualify as 'attacks' and are subject to all IHL rules on the conduct of hostilities.

Different types of cyber operations exist and **respect for the principle of distinction can be ensured in a number of ways**. For instance, if a cyber operation is carried out by operators who enter a target and carry out an operation against this target, the operators will normally know where they are and what they are doing. Thus, they can respect the principle of distinction. In other cases, operations may be carried out by using malware or other cyber tools. From a technological perspective, cyber tools can be programmed and used to target and harm only specific objects and to not spread or cause harm indiscriminately. However, the interconnectivity that characterises cyberspace means a cyber attack on a specific system may also spread to various other systems, for instance if a tool is designed to do so or is not sufficiently tested. As a result, there is a real risk that cyber tools are not designed or used – either deliberately or by mistake – in compliance with IHL.

In light of these risks, those who are planning or conducting cyber operations must do everything feasible to verify that targets are military objectives.[8] This should include, for example, a careful assessment of the targeted environment and the impact that a cyber operation will likely have; the testing of cyber tools in ICT environments similar to the ones targeted; and the use of technical measures such as 'system-fencing', 'geo-fencing', or 'kill switches' that may prevent or stop cyber tools from spreading and causing damage indiscriminately.[9]

Many of the IHL rules on the conduct of hostilities, including several rules stemming from the principle of distinction,[10] apply to – and therefore limit – only cyber operations that qualify as 'attacks' under IHL ('acts of violence against the adversary, whether in offence or in defence').[11] In the context of cyber operations, the IHL notion of attack is commonly understood as operations that may reasonably be expected to cause injury or death

6 ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015.

7 Additional Protocol I (1977), Article 51(4); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 11 and 12.

8 Additional Protocol I (1977), Article 57(2)(a)(i); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rule 16.

9 'System-fencing' means preventing malware from executing itself unless there is a precise match with the target system, 'geo-fencing' means limiting malware to only operate in a specific IP range, and 'kill switches' signify a way to disable malware after a given time or when remotely activated. For further details, see ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, 2021, pp. 26–27.

10 See, in particular, Additional Protocol I (1977), Articles 51(4) and (5)(b), 52, 54(c), and 57(1); ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 7–11, 14, 15.

11 Additional Protocol I (1977), Article 49. Note that IHL rules that provide specific protection for certain objects, such as medical facilities, impartial humanitarian organizations, or objects indispensable for the civilian populations enjoy protection against cyber operations beyond those qualifying as 'attacks'.

to people or damage or destruction to objects.[12] At present, States have taken different views on what types of effects caused by cyber operations may be considered 'damage' and qualify that operation as an 'attack' under IHL subject to all the rules limiting such operations.[13] If a narrow view is taken, this may mean that various cyber operations, such as those disrupting banking, civil administration, or private company IT systems without causing physical damage, may not be limited by the relevant IHL rules. This would be a real reason for concern. In the ICRC's view, during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means.[14]

During armed conflict, **cyber operations that do not amount to 'attacks' under IHL have limits, too**. For instance, the principle of necessity ↗, the obligation to take constant to spare the civilian population, civilians and civilian objects, the obligation to respect and protect medical facilities as well as humanitarian relief objects, and rules on the protection of objects indispensable to the survival of the civilian population apply to all military operations.[15] Moreover, at least States parties to Additional Protocol I have taken upon themselves the obligation to 'direct their operations only against military objectives'.[16] An interpretation of this rule that would permit directing cyber operations at civilian objects would be difficult to reconcile with the text of this treaty.

12 M. N. Schmitt and L. Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 92.

13 For an overview of positions taken by States on this subject, see Cyber Law Toolkit, 'Attack (international humanitarian law)'.

14 See ICRC, *International humanitarian law and cyber operations during armed conflicts: Position paper*, 2019, pp. 7–8.

15 See, in particular, First Geneva Convention (1949), Article 19, Additional Protocol I (1977), Articles 12, 54(2), 57(1), and 71, Additional Protocol II (1977), Articles 13(1), 14; ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 15, 25, 28, 29, 32, 54.

16 Additional Protocol I (1977), Article 48.

ICRC

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

03.2023