Humanity In War

WORKSTREAM 6

UPHOLDING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING ARMED CONFLICTS

BACKGROUND PAPER*

* This background paper was originally prepared for the first state consultation, with only minor corrections and updates made as of September 2025.

INTRODUCTION

The increasing use of information and communication technologies (ICTs) during armed conflicts raises significant humanitarian and legal questions. While it is widely accepted that international humanitarian law (IHL) imposes limits on the use of ICTs in armed conflict, the specificities of the ICT environment give rise to complex questions regarding its implementation. States have recognized the need for continued discussions on these questions. The ICT workstream is part of an ongoing effort to foster shared understandings.

I. THE USE OF ICTS IN ARMED CONFLICTS AND IHL: GLOBAL DISCUSSIONS AND EMERGING SHARED UNDERSTANDINGS

The application of international law, including IHL, to ICT activities has been the subject of multilateral discussions for nearly two decades. In 2021, the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE) noted by consensus that "international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognized the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict."[1] The Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025 echoed this conclusion in its reports.[2]

To date, and to our knowledge, 35 states have published individual national positions on how international law applies to cyber operations.[3] In addition, two regional organizations – the African Union and the European Union – published common positions or understandings on the application of international law to the use of ICTs, marking progress in building regional consensus and bringing the number of states opining on this subject to over 100. Emerging shared understandings include reaffirming the application of IHL principles and rules, including humanity, necessity, proportionality and distinction, to the use of ICTs during armed conflict. A growing number of states have also expressed their views on the protection afforded by IHL for, among others, civilians, civilian infrastructure, civilian data, medical personnel and facilities, and humanitarian activities and personnel against malicious ICT activities.

Building on this momentum, in October 2024 the 34th International Conference of the Red Cross and Red Crescent (34IC) – which brought together all states and all components of the

[1] *Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 2021, para. 71(f). Also see United Nations General Assembly Resolution 76/19, 2021, paras 2 and 3, adopted by consensus, which welcomes the consensus final report of the GGE and calls upon member states to be guided in their use of ICTs by the report.
[2] See Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, *First Annual Progress Report*, A/77/275, 2022, para. 15(b)(ii); *Second Annual Progress Report*, A/78/265, 2023, para. 29(b)(ii); *Third Annual Progress Report*, A/79/214, 2024, para. 36(b)(ii); *Draft Final Report,* A/AC.292/2025/CRP.1, 2025, para. 40(b)(ii).
[3] All individual national positions and common positions can be found at Cyber Law Toolkit, "Common and National Positions", at https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions.

International Red Cross and Red Crescent Movement (Movement) – adopted the resolution "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (ICT Resolution). The resolution urges states and parties to armed conflicts to protect the civilian population and other protected persons and objects in situations of armed conflict, including against the risks arising from malicious ICT activities. It also calls on states and parties to armed conflicts to uphold IHL protections for civilians, civilian critical infrastructure (including critical digital infrastructure, such as undersea cables and orbit communication networks), medical and humanitarian personnel and activities, and cultural property, including against the risks arising from ICT activities. It reiterates the prohibition on encouraging or inciting violations of IHL, and addresses issues relating to civilians conducting ICT activities, and private technology companies providing ICT services in the context of armed conflict.

Despite the progress noted above, it has been recognized that the specificities of the ICT environment raise questions on how principles and rules of IHL apply to ICT activities and that there is a need for further discussions.[4]

This workstream responds to this need and provides a dedicated space for focused and in-depth exchanges. In light of the human cost of the use of ICTs in armed conflict, the objective of the workstream is to foster shared understandings on the limits that IHL imposes on ICT activities in armed conflict to safeguard civilians from harm.

II. THE USE OF ICTS IN TODAY'S ARMED CONFLICTS AND THE HUMAN COST

The rapid digitalization of societies has brought significant benefits, enhancing social, economic and communication opportunities. In conflict-affected areas, reliable ICTs are critical for civilians to access essential goods and services, for governments to provide services, and for supporting medical and humanitarian activities, including those of the International Red Cross and Red Crescent Movement.

However, these advantages also come with risks, including those arising from an increase in the use of ICTs by states and non-state actors in armed conflicts. A number of states are developing ICT capabilities for military purposes, with growing deployment and use of ICTs as means or methods of warfare. Whereas the development and use of military ICT capabilities may offer belligerents the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure, the risk such activities pose to civilian populations and infrastructure remains a real concern. By using military ICT capabilities, processes controlled by computer systems can be triggered, altered or otherwise manipulated with the potential to cause significant harmful effects for civilians.

The use of ICTs targeting civilian critical infrastructure – such as nuclear facilities, power grids, water systems and telecommunications networks – can have "potentially devastating humanitarian consequences".[5] ICT activities can also disrupt e-governance services and

[4] *Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 2021, para. 71(f), and 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024, Resolution 2, "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (hereinafter ICT Resolution), preambular paragraph 19.

[5] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, *Final Substantive Report*, A/AC.290/2021/CRP.2, 2021, para. 18.

private sector operations, with societal and economic costs. These risks are compounded by the interconnectivity that characterizes cyberspace. ICT activities targeted at one system may have repercussions for various other systems, regardless of where those systems are located.

The health-care sector, along with humanitarian organizations, is especially vulnerable to ICT activities in armed conflict, which can disrupt life-saving medical operations, impair the operation of impartial humanitarian organizations and their personnel, and jeopardize the provision of essential assistance to those in need. For instance, the International Committee of the Red Cross (ICRC) and other components of the Movement, have been targeted by ICT activities.[6]

Additionally, the involvement of civilians in military activities through the use of ICTs during armed conflict has become more pronounced. States have tolerated, facilitated or encouraged civilian hackers and hacker groups to engage in ICT activities, targeting or affecting civilians and civilian objects associated with the adversary. Civilians have also been encouraged to report enemy troop movements, including via smartphone applications. Private companies are increasingly providing cybersecurity or other digital services to parties to armed conflict. If civilians are drawn closer to hostilities, they risk being exposed to harm. In addition, they are often not aware of the risks they are taking, the legal implications of their activities, or the IHL rules they have to respect.

Another dimension is the use of ICTs for spreading harmful information during armed conflict. While information operations have long been part of warfare and are not unlawful as such, the use of ICTs – especially on social media platforms or when coupled with artificial intelligence and other emerging technologies – amplifies the speed and scale of the spread of harmful information, including efforts to incite violence, expose detainees to public curiosity or undermine trust in humanitarian organizations.

States have acknowledged these developments and risks. The OEWG 2021-2025 has noted that states are developing ICT capabilities for military purposes, that the use of ICTs in conflicts is increasingly likely, and that ICTs have already been used in conflicts in different regions, with potentially devastating humanitarian consequences for civilians and civilian objects, as well as for international and humanitarian organizations.[7] The 34IC has also highlighted the potential harm to civilians caused by the use of ICTs by parties to armed conflicts, particularly where these means are directed against or incidentally affect civilian critical infrastructure and essential services, and the potential harm to impartial humanitarian organizations, hindering these organizations' access to affected populations.[8]

III. THE USE OF ICTS IN ARMED CONFLICTS: FRAMING THE LEGAL AND HUMANITARIAN QUESTIONS UNDER IHL

Existing IHL treaties and customary law provide protection for civilians and civilian objects against the dangers arising from ICT activities during armed conflict. As reiterated by the ICT Resolution, "in situations of armed conflict, IHL rules and principles – including the principle of distinction, the prohibition of indiscriminate and disproportionate attacks, the

[6] The 2022 data breach and repeated distributed denial-of-service attacks on the ICRC website highlight the need for robust data protection to safeguard sensitive information, ensure operational continuity and protect confidential humanitarian dialogue with parties to conflicts. See ICRC, "Cyber attack on ICRC: What we know", at https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[7] Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, *Draft Final Report,* A/AC.292/2025/CRP.1, 2025, paras. 15, 16 and 21.

[8] ICT Resolution, preambular paras 7 and 14.

obligations to spare the civilian population, civilians and civilian objects in the conduct of military operations, and to take all feasible precautions to avoid, and in any event minimize, incidental civilian harm, the prohibition of encouraging or inciting violations of IHL, and the prohibition of acts or threats of violence, the primary purpose of which is to spread terror among the civilian population – serve to protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities".[9]

Building on the above, the key legal issues below, relating to the most pressing humanitarian concerns, are proposed for further discussion.

I. PROTECTING CIVILIANS AND OTHER PROTECTED PERSONS AND OBJECTS FROM THE DANGERS ARISING FROM ICT ACTIVITIES DURING ARMED CONFLICTS

Protecting civilian populations from the effects of ICT operations during armed conflicts and the notion of attack under IHL

ICT operations have the potential to disable or physically damage industrial facilities, communication networks and other elements of a state's critical infrastructure. Such operations can also directly or indirectly cause injury or death to civilians – including by disrupting the functioning of essential services. These risks are compounded by the interconnectivity of digital space. While ICT operations that result in physical damage have received specific attention, the recent uses of ICTs, including in armed conflicts, have shown that even in the absence of physical damage, ICT operations can severely disrupt civilian infrastructure and interrupt the delivery of essential services. In fact, this constitutes one of the most important ICT risks for civilians during armed conflict.

The purpose of the IHL rules governing the conduct of hostilities is to ensure respect for and protection of the civilian population and civilian objects.[10] Most rules stemming from the principles and rules governing the conduct of hostilities, notably distinction, proportionality and precautions – which provide general protection for civilians and civilian objects – apply only to operations or activities that qualify as "attacks", as defined in IHL, i.e. "acts of violence against the adversary, whether in offence or in defence".[11] The question of how the notion of "attack" is interpreted with regard to the use of ICTs during armed conflict, in particular to ICT operations that disable civilian objects without causing physical damage, is therefore essential, as this determines whether these rules apply, and thus whether civilians and other protected persons and objects are protected against the dangers arising from such operations.

It is well established that the notion of violence in the definition of "attack" under IHL can refer to either the means used or the consequences or effects produced. An operation that causes violent effects qualifies as an attack, even if the means used are not violent in themselves.[12]

It is also widely accepted that an ICT operation that is expected to cause death or injury to a person, or damage or destruction to an object, constitutes an attack under IHL.[13] It is

[9] ICT Resolution, para. 4.
[10] Additional Protocol I of 8 June 1977, Article 48 and titles of Part IV and Section I.
[11] Additional Protocol I, Article 49(1). There are a few IHL rules that apply to all military operations, including those carried out through ICT activities. See, for example, Additional Protocol I, Articles 48, 51(1) and 57(1).
[12] Y. Sandoz, C. Swinarski and B. Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva/Martinus Nijhoff, Leiden, 1987 (hereafter ICRC, Commentary on the Additional Protocols), para. 1881 on Article 49(1) of Additional Protocol I states that "there is an attack whenever a person is directly endangered by a mine laid", which is an interpretation consistent with the consequence-based approach. Another generally accepted example is that the use of a chemical or biological agent would constitute an attack due to the violent effects it causes, even if the means of delivering such agents may not be violent.
[13] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2015, pp. 41–42.

commonly understood that this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an operation, for example the death of patients in intensive-care units caused by an ICT operation against an electricity network that results in cutting off a hospital's power supply.[14]

Beyond this, further discussion among states is needed on which IHL rules limit ICT operations that affect the functionality of ICT systems without necessarily causing physical damage or destruction to an object or injury or death to a person, including whether they qualify as "attacks" under IHL.

From a contemporary warfare perspective, recognizing as an attack under IHL, an ICT operation that disables an object without causing physical damage, is crucial for the protection of civilians and civilian objects against ICT activities during armed conflict. A restrictive interpretation of the notion of attack, that excludes certain ICT activities from the protection afforded by key IHL rules on the conduct of hostilities, would be difficult to reconcile with the object and purpose of IHL, and with the need to ensure that its protective framework remains effective in light of the evolving means and methods of warfare. It is essential in this regard that states find a common understanding to protect civilians and civilian objects against the effects of harmful use of ICTs during armed conflict.

Civilian data and the notion of civilian objects under IHL

Civilian data – such as medical data, biometric data, social security data, tax records, bank accounts, humanitarian data, companies' client files or election lists and records – are an essential component of digitalized societies. Such data are key to the functioning of most aspects of civilian life, be it at the individual or societal level. There is increasing concern about protecting such data. Deleting or tampering with civilian data can quickly bring government services and private businesses to a standstill and may cause more harm to civilians than the destruction of certain physical objects. In addition, stealing or leaking civilian data can expose individuals and communities to serious risks of harm.

With regard to data belonging to certain categories of persons and objects that enjoy specific protection under IHL, the protective rules are comprehensive. For example, the obligation to respect and protect medical personnel, units and transports, humanitarian personnel and objects, and objects indispensable for the survival of the civilian population extend to their data.[15] Beyond that, however, it is important to better understand the extent to which civilian data are protected by existing IHL rules,[16] in particular whether data constitute objects as understood under IHL, in which case ICT operations against data (such as damaging or deleting them) would notably be governed by the principles of distinction, proportionality and precaution.

In this respect, some states have taken the view that the protection of civilian objects extends to all types of civilian data; some seem to draw a difference between "content data" and

[14] ICRC, *Position Paper on International Humanitarian Law and Cyber Operations during Armed* Conflicts, 2019, p. 7. For an overview of positions taken by states, see Cyber Law Toolkit, "Attack (International Humanitarian Law)", at https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).
[15] See the next section of this paper, "Specifically protected persons and objects under IHL".
[16] These include IHL principles and rules on the conduct of hostilities. Other relevant rules may include the protection of cultural property, the protection of property against seizure and destruction, and the prohibition of pillage.

other data; while others have taken the view that digital data cannot generally be considered to be objects under IHL.[17]

Further discussion among states is needed to build shared understandings on this critical issue. From a humanitarian perspective, the assertion that an operation designed or expected to delete or tamper with civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL. Logically, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to the information stored in the data.

Specific protections for persons, objects and activities under IHL

Some rules of IHL afford specific protection to certain categories of persons, objects and activities, beyond the prohibition of attacks, including with regard to ICT activities.

For example, belligerents must respect and protect medical personnel and facilities at all times,[18] including the requirement not to unduly interfere with the functioning of medical services and take feasible measures to protect them against harm or interferences from private persons not attributable to parties to armed conflict.[19] Likewise, humanitarian personnel and objects used for humanitarian operations must be respected and protected;[20] and parties to armed conflicts must allow and facilitate impartial humanitarian activities during armed conflict subject to their right of control.[21] For both medical services and humanitarian personnel and objects, specific protection extends to communications and data.[22]

To strengthen the protection of medical services and humanitarian activities against ICT-related risks, further discussion may focus on how to operationalize such protection. One avenue is the effort led by the ICRC to develop a digital emblem – that is, a means of identifying the digital infrastructure and data of organizations and entities entitled to display the distinctive emblems recognized under IHL.[23] The ICT Resolution, taking note of the ongoing work of the ICRC in consultation with states and components of the Movement, encourages further work and consultations, including to study possible legal and diplomatic avenues for the potential use of a digital emblem.[24]

Furthermore, ICT activities that "destroy, remove or render useless" objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation works, fall within the scope of the special protection accorded to such objects under IHL, irrespective of whether they qualify as attacks.[25] The special protection extends to ICT

---

[17] For an overview of positions taken by states, see Cyber Law Toolkit, "Data as a military objective", at https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL.

[18] See, for instance, First Geneva Convention of 12 August 1949, Article 19; Second Geneva Convention of 12 August 1949, Article 12; Fourth Geneva Convention of 12 August 1949, Article 18; Additional Protocol I, Article 12; Additional Protocol II of 8 June 1977, Article 11; ICRC, Customary IHL Study, at https://ihl-databases.icrc.org/en/customary-ihl/rules (hereafter ICRC, Customary IHL Study), Rules 25, 28 and 29.

[19] ICRC, Commentary on the Additional Protocols, para. 517 on Article 12 of Additional Protocol I, and ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd ed., ICRC, Geneva / Cambridge University, Cambridge, 2016 (hereafter ICRC, Commentary on the First Geneva Convention, 2016), para. 1799 on Article 19.

[20] Additional Protocol I, Articles 70(4) and 71(2); ICRC, Customary IHL Study, Rules 31 and 32.

[21] See Fourth Geneva Convention, Article 23; Additional Protocol I, Article 70(2); Additional Protocol II, Article 18(2); ICRC, Customary IHL Study, Rules 55.

[22] ICRC, Commentary on the First Geneva Convention, 2016, para. 1804 on Article 19.

[23] The Digital Emblem project is a stand-alone project led by the ICRC in consultation and engagement with states and components of the Movement. The discussion within this workstream will not focus on this project.

[24] ICT Resolution, preambular para. 15 and operative para. 12.

[25] Examples of such objects include, but are not limited to, "foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works." Additional Protocol I, Article 54(2); Additional Protocol II, Article 14; ICRC, Customary IHL Study, Rule 54. See also ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, pp. 46–47.

infrastructure that is itself "indispensable" to the functioning of such objects. Further discussion is needed on measures to operationalize such protections.

Finally, IHL rules prohibit sexual violence and afford specific protections to certain categories of persons, including though not limited to women, elderly, persons with disabilities and children (for instance, against their unlawful recruitment or use in hostilities).[26] Further discussion is needed, among other issues, on practical measures to ensure compliance with these rules, including when facilitated by ICTs.

II. PROTECTING CIVILIANS AND OTHER PROTECTED PERSONS FROM INFORMATION SPREAD IN VIOLATION OF IHL DURING ARMED CONFLICTS

States and non-state armed groups are spreading digital information for a variety of purposes, including when carrying out information or psychological operations. Some operations aim to reduce the risk of harm to humans during armed conflicts, for example by giving civilians an effective advance warning of an attack or by helping to direct them to safety. Others are designed to cause confusion or harm, to deceive an adversary or to support the military or political objectives of a party to the conflict. In today's armed conflicts, ICT activities are used to spread information in violation of IHL. Information spread through ICT activities can contribute to or encourage violence, cause lasting psychological harm, undermine access to essential services and disrupt the operations of humanitarian organizations, which may undermine trust in these organizations.

IHL contains several specific rules that impose limits on spreading information, including through digital means, in particular the following:

- Civilian and military officials of a party to an armed conflict must not encourage IHL violations, including through digital platforms.[27] The ICT Resolution further reaffirms the prohibition of encouraging or inciting violations of IHL through digital means.[28]
- Prisoners of war and other protected persons under IHL must be protected against public curiosity.[29] Public sharing by authorities of data, images and videos of prisoners of war and others deprived of their liberty, subject to limited exceptions, would violate this rule, and states must protect against sharing by private entities as well.[30]
- Threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited under IHL.[31]
- False information spread by parties to armed conflict to obstruct medical or humanitarian work is incompatible with the obligations to respect and protect medical and humanitarian personnel and their activities.[32]

[26] Fourth Geneva Convention, Article 27(2); Additional Protocol I, Articles 76(1) and, 77(1) and (2); Additional Protocol II, Article 4(3)(c); ICRC, Customary IHL Study, Rules 134 to138.
[27] Fourth Geneva Convention, Common Article 1; ICRC, Customary IHL Study, Rule 139.
[28] ICT Resolution, para. 4.
[29] See, for example, Third Geneva Convention of 12 August 1949, Article 13 and Fourth Geneva Convention, Article 27.
[30] For further discussion on this issue, see, for example, ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War, 2nd ed.*, ICRC, Geneva, 2020 (hereafter ICRC, Commentary on the Third Geneva Convention, 2020), paras 1623–1632.
[31] Additional Protocol I, Article 51(2); Additional Protocol II, Article 13(2); ICRC, Customary IHL Study, Rule 2.
[32] This, of course, is different from criticism or the expression of anger by authorities or beneficiaries directed at the medical services or humanitarian organizations, which is not *prima facie* unlawful.

- Information spread for the purpose of child recruitment, or propaganda aimed at enlisting protected persons in occupied territories, into the armed forces is unlawful.[33]

Given the above-mentioned risks of harm for civilians and other protected persons under IHL, further discussion is needed to develop shared understandings on how IHL applies to information spread, ensuring the effective protection of all protected persons and objects under IHL.

III. THE RISK OF HARM ARISING FROM THE MILITARY USE OF CIVILIAN ICT INFRASTRUCTURE AND THE INVOLVEMENT OF CIVILIANS IN ICT ACTIVITIES DURING ARMED CONFLICTS

The military use of civilian ICT infrastructure and the resulting impact on its protection under IHL

Except for certain military networks, cyberspace is predominantly civilian. However, the interconnectedness of civilian and military networks and the use of civilian ICT infrastructure by the military pose specific challenges for its protection.

If civilian ICT infrastructure – including infrastructure provided by technology companies – is used for military purposes (in which case such infrastructure is sometimes referred to as "dual-use"), it risks becoming a military objective under IHL and losing its protection against attack.[34] In such cases, civilians and civilian objects in physical proximity, digitally connected to or dependent on such infrastructure, risk incidental harm.

However, not every military use turns a civilian object into a military objective under IHL; this occurs only when the use meets the criteria for a military objective as defined by IHL. Furthermore, even if a belligerent considers a civilian or civilian object to have lost protection due to involvement in ICT operations, any attack remains subject to the prohibitions on indiscriminate and disproportionate attacks and the obligation to take all feasible precautions. Additionally, certain specifically protected objects may not be attacked or may be subject to stricter limitations, even when they fulfil the definition of a military objective.

To protect civilian populations and essential civilian services relying on ICT infrastructure, further discussion is necessary to determine when military use of predominantly civilian ICT infrastructure turns it into a military objective, and to identify and implement other feasible protective measures. For instance, the ICRC has called on states to, whenever feasible, segment – that is physically or technically separate – ICT infrastructure (or parts thereof) used for military purposes from that used for civilian purposes.[35] It is also essential to ensure that any specific protection granted under IHL is respected.

---

[33] Regarding child recruitment, see ICRC, Customary IHL Study, Rule 136 and obligations under the Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict of 25 May 2000. Regarding protected persons in situations of occupation, see Fourth Geneva Convention, Article 51.

[34] Dual-use objects may become military objectives if they, under the circumstances ruling at the time, fulfil the definition under Article 52(2) of Additional Protocol I: "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage".

[35] One example would be when deciding whether to store military data on a non-segmented commercial cloud, a segment of a commercial cloud or dedicated military digital infrastructure, military planners and operators should not use the non-segmented commercial cloud. See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, pp. 53–54.

The involvement of civilians in ICT activities during armed conflicts

In today's armed conflicts, several trends pose risks for civilians: civilian hackers increasingly target civilian objects in ICT operations; parties to armed conflict encourage civilians to collect militarily relevant information through digital means, exposing them to attacks; and civilian technology companies providing ICT services and infrastructure to armed forces risk losing their legal protection.

IHL is built on the cardinal principle of distinction. The growing civilian involvement in ICT operations and the military use of civilian ICT infrastructure risk undermining the protection that this foundational principle is meant to provide to civilians, including against being misidentified as lawful targets.

Individuals and groups, including hackers and technology company employees, conducting ICT activities in the context of armed conflicts must comply with the limits that IHL sets for such activities,[36] and be aware of the risks involved. In exceptional cases, civilian involvement in ICT activities may amount to "direct participation in hostilities", meaning that a civilian loses the protection against attack for such time only as this is the case. However, in case of doubt, IHL requires that a person be considered civilian and protected as such.[37]

States' responsibility to disseminate IHL and to prevent and suppress IHL violations

With regard to civilian involvement in ICT activities during armed conflict, it should be noted that states have undertaken to respect and ensure respect for IHL. If civilian hackers, private companies or other private individuals or entities act under the instruction, direction or control of a state, that state is internationally legally responsible for any conduct of those individuals that is inconsistent with the state's international legal obligations, including IHL.[38]

Even if the conduct of civilians is not attributable to a party to armed conflict, states are nonetheless obliged to ensure respect for IHL. At a minimum, parties to an armed conflict must not encourage, aid or assist civilians involved in ICT activities to violate IHL,[39] for example by encouraging civilians to direct ICT operations against civilian objects. Furthermore, states must disseminate knowledge of IHL, prevent and suppress violations of IHL, and investigate and prosecute war crimes, including those committed by the civilian population.[40]

---

[36] With regard to civilian hackers operating in the context of armed conflicts, these limits have been summarized in ICRC, "Eight rules for 'civilian hackers' during war, and four obligations for states to restrain them", at https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them. On the relevance of IHL to private businesses, see more generally, ICRC, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law*, 2024.

[37] Additional Protocol I, Article 50(1). If there is a risk that children may be drawn into hostilities through ICT activities and considered as directly participating in hostilities, belligerents have an additional obligation to prevent the involvement of children under 15 or 18, depending on the applicable legal framework.

[38] Under public international law, a state is responsible for the conduct of private persons, groups, or entities – including civilian hackers or hacker groups – if they are "empowered by the law of that state to exercise elements of the governmental authority", or "in fact acting on the instructions of, or under the direction or control of, that state". See International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, 2001, Articles 5 and 8.

[39] ICRC, Commentary on the Third Geneva Convention, 2020, para. 191 on Article 1.

[40] ICRC, Commentary on the Third Geneva Convention, 2020, para. 183 on Article 1.