HUMANITARIAN LAW & POLICY

From hackers to tech companies: IHL and the involvement of civilians in ICT activities in armed conflict

November 4, 2025, Accountability / Analysis / Communications / Conduct of Hostilities / Generating Respect for IHL / IHL / Law and Conflict / New Technologies / Scope of application

10 mins read

Tilman Rodenhäuser
Thematic Legal Adviser, ICRC

Samit D'Cunha
Legal Adviser, ICRC

Laurent Gisel
Head of the Arms and Conduct of Hostilities Unit, ICRC

Anna Rosalie Greipl
Researcher, The Academy of International Humanitarian Law and Human Rights (Geneva Academy)

Marco Roscini
Professor of International Law, the University of Westminster

Picture a potential future armed conflict: missiles and drones crowding the skies, uncrewed vehicles rolling across borders, and governments scrambling to coordinate their defences. Their conclusion:

Every citizen is needed. Some collect and relay information about the approaching enemy into an artificial intelligence (AI) platform that supports military decision-making. Reservists join the ranks of the armed forces. Computer experts choose to contribute by conducting cyber operations aimed at disrupting military operations, sowing chaos among the civilian population, and harming the enemy's economy. As the militaries on both sides rely heavily on digital communication, connectivity, and AI, the armed forces call on tech companies to provide cybersecurity services, computing power and digital communication networks.

In this post, Tilman Rodenhäuser, Samit D'Cunha, and Laurent Gisel from the ICRC, Anna Rosalie Greipl from the Academy, and Professor Marco Roscini from the University of Westminster (and former Swiss IHL Chair at the Geneva Academy) present five key risks for civilians, along with the obligations of both civilians and states, related to the involvement of civilians in information and communication technology (ICT) activities in armed conflict.

Civilians have long been involved in activities closely linked to hostilities during armed conflict. With strategies such as '*total defence*' and 'comprehensive defence' – which entail mobilizing the 'whole of society' in the defence of a country – civilian involvement in armed conflict may become increasingly direct and widespread. Further catalyzing this shift, the rapid digitalization of our societies and the way in which wars are fought means the involvement of civilians in armed conflicts can take new forms, with the result that the related risks reach an unprecedented scale.

As part of a joint initiative, entitled '*Digitalization of Conflict: Humanitarian Impact and Legal Protection*', by the International Committee of the Red Cross (ICRC) and the Geneva Academy of International Humanitarian Law and Human Rights (the Academy), we conducted in-depth research and consulted experts in an effort to explore and clarify how international humanitarian law (IHL) addresses the involvement of civilians in cyber and other digital activities during armed conflict. Our report on the issue was published today. Here are some of our key findings, and recommendations for civilians, states, and tech companies.

First, states should avoid involving civilians in armed conflict.

The digitalization of our societies is contributing to a growing involvement of civilians in cyber operations and other digital activities during armed conflicts. Such involvement takes many forms. Civilians may become involved as individuals by conducting a cyber operation against what they regard as part of the adversary's war effort. Civilians have also engaged in defensive digital activities or have been involved in the gathering and sharing of information of military value.

The involvement of civilians can have serious implications for civilian populations. It risks generating confusion about who or what is 'civilian' and thus protected from attack, and who or what is a 'military objective' and may therefore be targeted. As a result, it increases the risk of both erroneous and unlawful attacks. To avoid such risks:

- States should – to the extent feasible – avoid involving civilians in activities that bring them close to hostilities, and if they decide to involve them, give due consideration to the risks this would expose civilians to.
- If states intend to use civilians in activities that bring them close to hostilities, they should integrate these civilians into their armed forces, or at least inform them of relevant risks and obligations arising from their involvement in the hostilities.

Second, civilians must know and respect IHL.

Threat analysts have counted dozens of civilian hacker groups conducting cyber operations in the context of recent armed conflicts. Some of these 'hacktivists' or hacker groups are professionally organized or even state-sponsored. Others operate independently and have varying degrees of internal organization. Still others are loosely organized collectives. These groups

often direct their cyber operations not against military objectives, but against the civilian segments of societies – such as banks, internet service providers, transport and energy infrastructure, online pharmacies, hospitals, or civilian government services.

IHL applies to the acts of civilians when those acts take place in the context of, and are associated with, an armed conflict. This is regardless of whether those activities are conducted by individual civilian hackers, civilians acting as part of a hacker group, or employees of technology companies. Accordingly,

- if civilians conduct cyber operations in the context of an armed conflict, they must seek information about the limits that IHL imposes on such operations, develop a sufficient understanding of these limits, and respect them.
- This includes, in particular, the principles of distinction, proportionality and precaution, and the specific protection afforded to certain categories of persons and objects, as recalled, for example, in the ICRC's '*8 Rules for Hackers During War*'.

Third, states must make IHL known and suppress violations.

In times of armed conflict, parties to armed conflict – whether states or non-state armed groups – must respect IHL and ensure respect for it by any person or group that forms part of their armed forces or acting on their instructions or under their direction or control. In other words, under international law, states cannot escape responsibility by having their organs or agents pretend to operate as hacktivists and thus independently from the state, and states must not aid, assist, or encourage civilians to violate IHL.

Furthermore, states have a due-diligence obligation to prevent IHL violations by all civilians within their jurisdiction, including civilian hackers, hacker groups, or tech-companies staff. This long-standing obligation is particularly relevant for the involvement of civilians in armed conflicts. Practical measures that can be taken to this effect include the following:

- States should make IHL known, as necessary and feasible, to civilian hackers, hacker groups, and employees of private technology companies, demanding that they respect IHL. Some states have asked their citizens to refrain from conducting cyber operations related to armed conflicts and other states have more generally informed their citizens of the practical and legal risks arising from taking part in the hostilities.
- In all cases, states have committed to taking the measures necessary to suppress IHL violations and prosecute those who commit war crimes. This requires having relevant legislation in place and enforcing it.

Fourth, tech companies should know the risks associated with providing services to the parties to an armed conflict.

As private technology companies increasingly operate in contexts affected by armed conflicts – including by offering products or services to parties to conflicts – they must be aware of the legal and practical implications. IHL provides important legal protection for the civilian personnel and property of tech companies: they must not be attacked. Such protection can, however, be lost if the company's personnel carry out certain activities or if the company's property is used in certain ways. For instance, where specific tech company infrastructure or services are used by a warring party to make an effective contribution to military action and its total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage to the adversary, it becomes a military objective. As tech companies provide the backbone of today's digitalized societies, attacks against them will likely affect not only the company but also essential services for civilian populations.

If private technology companies provide digital services to the parties to an armed conflict, these companies should

- familiarize themselves with IHL, understand how their services and activities may expose their staff, assets, and customers to harm, and take effective measures to minimize those risks.

- to the extent feasible, segregate the parts of their assets that are used by militaries from those used by civilian customers so to prevent or at least minimize incidental damage to civilian objects and persons resulting from an attack on a military objective.

Fifth, civilians must know the risks.

Civilians must be aware of the risks of harm arising from conducting cyber operations and other digital activities during armed conflicts. Under IHL, civilians lose protection against attack only if they directly participate in hostilities, and only for such time as they do so. Parties to armed conflict must carefully assess when this might be the case and, in case of doubt, must act on the presumption that civilians retain their full protection. Under IHL, a civilian hacker conducting cyber operations to disrupt a party to the conflict's military operations might directly participate in hostilities and lose protection against attack, although only for the duration of the participation. In contrast, although the widespread use of smartphones has enabled civilians to gather and share militarily relevant information with armed forces, the mere fact of a civilian using a smartphone near a site of hostilities, even if seemingly taking a picture or video of the armed forces, cannot, without more, be considered a direct participation in hostilities.

Assessing whether a civilian loses protection against attack is legally and factually complex. In practice, effective precautions will provide the best protection. Thus:

- Civilians must be aware — and states should make them aware — that hacking in support of a party to an armed conflict and to the detriment of an adversary, or collecting militarily relevant information for a belligerent, might put them at risk of real harm.
- In case of doubt, IHL *requires* the parties to an armed conflict to presume that civilians are protected against attack. In practice, it will be difficult for an attacker to determine the purpose for which individuals are using their phones in areas where hostilities are taking place; accordingly, they should refrain from attacking.

Key takeaways and implications

As 'total' or 'comprehensive' defence strategies reemerge, the current trend of involving civilians in activities closely linked to hostilities is likely to grow. The digitalization of our societies and of contemporary armed conflicts contributes to the acceleration of this trend, which raises important legal questions about the protection of civilians involved in armed conflict and their obligations under IHL.

Our joint report presents in-depth legal analysis on this subject and presents a set of actionable recommendations, in particular for states. It is also hoped that this report will contribute to a better understanding of the application of IHL in an ICT environment, clarify legal questions, and, ultimately, prevent harm.

Some of the issues discussed in our report have been addressed by states and members of the International Red Cross and Red Crescent Movement in the '*ICT Resolution*' of the 34th International Conference of the Red Cross and Red Crescent; however further work among states and experts is needed, including through ongoing discussions (which will continue into 2026) in the ICT Workstream of the *Global IHL Initiative*.

See also:

- Jean-Marie Henckaerts, *Protecting civilians in good faith: the updated Commentary on the Fourth Geneva Convention*, October 21, 2025
- Ruben Stewart, *The shifting battlefield: technology, tactics, and the risk of blurring lines in warfare*, May 22, 2025
- Cléa Thouin, *Offline and in danger: the humanitarian consequences of connectivity disruptions*, July 1, 2025

- Tilman Rodenhäuser and Mauro Vignati, *8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them*, October 4, 2023
- Kubo Mačák & Tilman Rodenhäuser, *Towards common understandings: the application of established IHL principles to cyber operations*, March 7, 2023

Tags: AI decision support systems, armed conflict, Artificial Intelligence, civilian hackers, Civilians, Cyber and Information Operations, direct participation in hostilities, Geneva Conventions, hacktivists, information and communication technology (ICT), international humanitarian law, Legal Review of Weapons, Means and Methods of Warfare, modern warfare, Respect for IHL

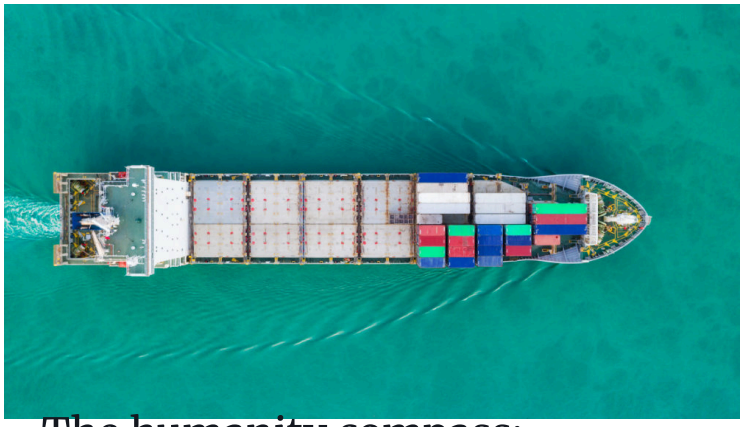
ICRC engagement with armed groups in 2025

14 mins read

Accountability / Analysis / Communications / Conduct of Hostilities / Generating Respect for IHL / IHL / Law and Conflict / New Technologies / Scope of application

Matthew Bamber-Zryd

In line with its mandate, the ICRC engages with all parties to an armed conflict, ...



The humanity compass: navigating the protection of civilians in naval warfare

13 mins read

Accountability / Analysis / Communications / Conduct of Hostilities / Generating Respect for IHL / IHL / Law and Conflict / New Technologies / Scope of application

André Smit & Kelisiana Thynne

The law of naval warfare is a complex collection of international laws, developed in an ...