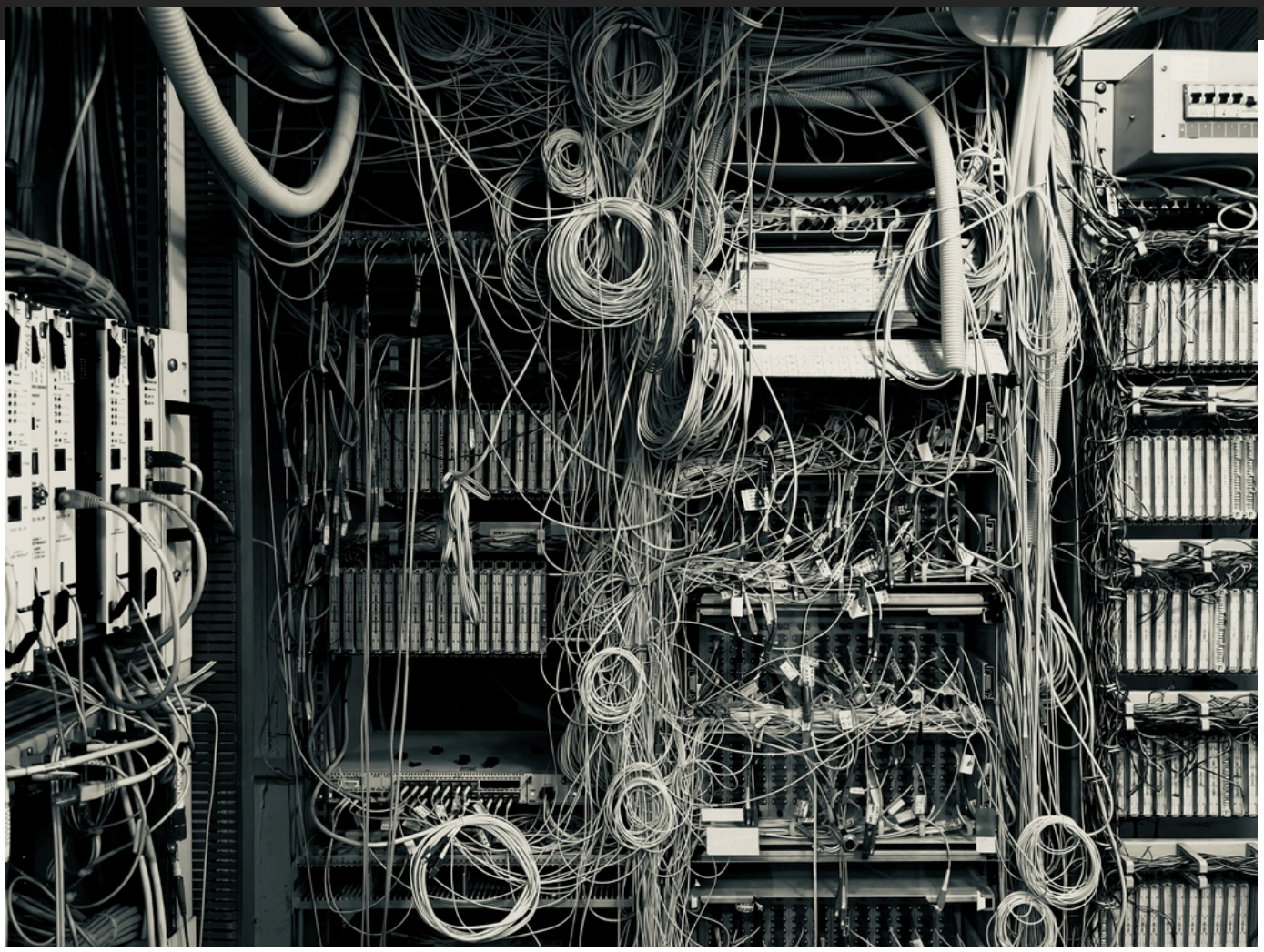
HUMANITARIAN LAW & POLICY

Upholding IHL protections against the risks of ICT activities in armed conflict

April 23, 2026, Analysis / Conduct of Hostilities / Cyber / IHL / New Technologies / Technology in Humanitarian Action

14 mins read

Wen Zhou
Legal Adviser, ICRC



Across the world, essential civilian services increasingly depend on information and communication technologies (ICTs). These same technologies are also reshaping the conduct of armed conflict. As warfare becomes more digitalized, a critical question emerges: how can civilians be protected in an interconnected battlespace? Ensuring the faithful implementation of international humanitarian law in relation to ICT activities is central to this challenge.

In this post, Wen Zhou, ICRC Legal Adviser with the Global Initiative to Galvanize Political Commitment to International Humanitarian Law (Global IHL Initiative), draws on discussions under the ICT workstream of the Initiative to highlight key humanitarian and legal questions arising from ICT activities in armed conflict, and to reflect ongoing efforts by states and other stakeholders to uphold the protections afforded by IHL and strengthen its implementation in practice.

The humanitarian implications of ICT activities during armed conflict extend far beyond the digital environment. In highly interconnected societies, disruptions to ICT systems can have immediate and far-reaching consequences for civilians.

Electricity networks, telecommunications, financial systems, healthcare, public services and humanitarian operations all depend on the availability and integrity of ICTs. When these systems are disrupted during armed conflict, essential services may fail, affecting the civilian populations that rely on them.

At the same time, the use of ICTs in armed conflict has increased significantly, by both states and non-state actors. A growing number of states are developing ICT capabilities for military purposes, with their use as means or methods of warfare becoming increasingly common. While such capabilities may allow belligerents to achieve military objectives without necessarily causing physical damage, they also create new risks of harm for civilians and civilian infrastructure, compounding the destruction already caused by bombardment and other traditional means and methods of warfare.

International humanitarian law (IHL) provides the framework to address these risks. As a body of law that seeks, for humanitarian reasons, to limit the effects of armed conflict, IHL applies to all forms of warfare and to all kinds of weapons, whether past, present or future (para 86, *Legality of the Threat or Use of Nuclear Weapons*, International Court of Justice). Its principles and rules "*serve to protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities*". ICT activities conducted in the context of and associated with an armed conflict must therefore comply with IHL at all times.

International discussions on ICTs and IHL and the ICT workstream of the Global IHL Initiative

The growing importance of ICT activities in armed conflict has prompted increasing attention among states and other stakeholders. Discussions on how international law, including IHL, applies to such activities are not new. They build on decades of work at national, regional and multilateral levels, including within the United Nations and other expert processes. These include, among others, the work of successive UN Groups of Governmental Experts and Open-Ended Working Groups (*here* and *here*), the resolution of the 34th International Conference of the Red Cross and Red Crescent entitled *"Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict"*, *national and common positions*, and most recently the Global Mechanism on developments in the field of ICTs, whose organizational session took place last month, as well as academic and expert initiatives such as the *Tallinn Manual process* and the ICRC's *Global Advisory Board*.

Despite this progress, the specificities of the ICT environment continue to raise questions about how IHL principles and rules apply in practice, highlighting the need for further discussion.

In this context, the ICT workstream of the *Global IHL Initiative* was established to provide a dedicated space for states and other stakeholders to examine these issues in a focused manner, building on existing discussions and complementing ongoing multilateral processes. As one of the seven thematic workstreams under the Global IHL Initiative, it contributes to the Initiative's overarching objective of making respect for IHL a global political priority and strengthening protection on the ground by providing concrete guidance on the implementation of existing IHL in a manner consistent with its protective purpose.

Against this backdrop, several key humanitarian and legal issues arising from ICT activities in armed conflict merit closer examination: How to ensure that the protection afforded by IHL is effectively upheld in an increasingly digitalized battlefield? How do existing rules of IHL apply to ICT operations that disable systems without causing physical damage? How can civilian data and infrastructure be protected? What risks arise when civilian systems are used for military purposes, and how can they be mitigated? What are the implications of increasing civilian involvement in ICT activities? How can medical services and humanitarian activities be safeguarded against ICT activities? And how should the spread of information in violation of IHL be addressed?

The following sections highlight some of the issues currently under consideration, without seeking to provide definitive answers.

When disabling systems harms civilians: how IHL provides protection

Most ICT operations in contemporary armed conflicts do not result in physical damage comparable to that caused by missiles or drones. Yet in practice, disabling systems, such as hospital networks, electricity grids or communications infrastructure, can have significant consequences for civilians who depend on them.

When ICT operations are conducted in the context of and associated with an armed conflict, the IHL rules governing the conduct of hostilities applicable to such operations depend, in part, on whether they qualify as "attacks" under IHL.

Against this background, discussions increasingly reflect the view that ICT operations expected to cause death or injury to persons, or damage or destruction to objects, qualify as attacks under IHL (see e.g. Tallinn Manual 2.0, Rule 92 and *some states' views*). An important question in this regard is how IHL applies to ICT operations that disable systems without causing physical damage and in particular whether the specific rules governing attacks under IHL apply to such operations.

As noted in the past (*here* and *here*), overly restrictive interpretations of the notion of attack risk limiting the protection afforded by IHL in ways that may be difficult to reconcile with its object and purpose.

Data at risk: when compromise leads to harm

Modern societies are increasingly digitalized, and their functioning today depends heavily on digital data. E-governance, financial systems, social services and humanitarian activities all rely on its availability and integrity.

When data is deleted, altered or rendered inaccessible during armed conflict, the consequences can be immediate: essential services may be disrupted and institutions on which civilians depend undermined. The theft or unauthorized disclosure of civilian data can likewise expose individuals and communities to serious risks of harm.

This raises a key question: how does IHL protect data?

While no IHL treaty explicitly refers to data, discussions to date have recognized that existing IHL rules protecting certain objects and activities extend to the data on which they rely (see e.g. *Tallinn Manual 2.0*, Rule 132 commentary, para 3 and some states' views *here*, *here* and *here*). Beyond that, a central issue in ongoing discussions is how the principles governing the conduct of hostilities apply when operations are directed against or affect data (see *some states' views*).

In today's world, where essential data is increasingly stored in digital rather than physical form, ensuring the protection of civilian data from deletion or manipulation under IHL is a humanitarian imperative. Excluding such data from protection would risk creating a significant protection gap.

Civilian ICT infrastructure: interconnected risks, cascading effects

Civilian ICT infrastructure, such as telecommunications networks, cloud services and data centres, underpins essential services across society. Yet in practice, it is often used, at least in part, for military purposes during armed conflict.

This creates structural risks. Not every such use renders ICT infrastructure a military objective, but it may increase the likelihood of it being targeted, exposing civilians who rely on it to incidental harm. Because ICT systems are highly interconnected, the effects of attack can cascade across sectors and borders.

IHL provides a framework to address these situations, but its application requires careful operationalization. Where military use of civilian ICT infrastructure renders it, or parts of it, a military objective, the IHL prohibitions on indiscriminate and disproportionate attacks as well as the principle of precautions apply, alongside any special protections afforded under IHL depending on the infrastructure concerned (see discussion below)

Reducing the risks of harm arising from the military use of civilian ICT infrastructure is not only a matter of compliance during operations, but also of preparation in peacetime. This includes clarifying when military use may render civilian infrastructure a military objective, and implementing all feasible precautionary measures, such as separating components used for military purposes from those serving only civilian functions.

Civilians in the digital battlespace: blurred lines, real consequences

Another feature of contemporary conflicts is the *growing involvement of civilians in ICT activities*. From civilian hackers to personnel of technology companies, individuals are increasingly drawn into ICT activities linked to hostilities. Civilians engaging in such activities may expose themselves to harm, often without fully understanding the risks involved or the legal implications.

This trend raises important questions under IHL. Civilians who conduct ICT operations in the context of and associated with an armed conflict must respect IHL, as increasingly reflected in recent expert and policy discussions (e.g. ICC OTP *Policy on Cyber-Enabled Crimes*, para. 81). At the same time, questions arise as to what practical measures states can and must take to prevent and stop IHL violations committed by civilian hackers or hacker groups or by technology companies that may task their personnel to engage in such activities.

These developments highlight the importance of states and parties to armed conflict taking measures to address this phenomenon and mitigate the associated risks.

Technology companies: critical actors, growing responsibilities

Technology companies play a critical role in today's digitalized societies, including in armed conflict. They are often the main providers of ICT products and services, such as cloud storage, communication platforms and cybersecurity tools, which are essential to civilian life but also used by parties to armed conflict.

This reality creates both risks and responsibilities. Their infrastructure has been targeted in recent armed conflicts. The disruption or destruction of their services can have significant consequences not only for military but also for civilian users. These developments highlight the importance of responsible conduct by companies in this environment. This includes understanding how their services may be used, assessing associated risks, and considering measures to reduce harm to civilians and civilian infrastructure.

If companies work closely with parties to armed conflict, they should be aware that they may face legal and practical risks if their products and services are used in ways that facilitate violations of IHL. This underscores the need for clear policies and safeguards to ensure that their operations do not contribute to such violations.

Preserving special protections in relation to ICT activities

Certain persons, objects and activities benefit from special protection under IHL, and these protections remain fully relevant when it comes to the use of ICTs. A key question, however, is how these protections can be effectively operationalized in the ICT environment, including how they apply to the data and ICT systems on which such protected objects depend, and how this protection can be made effective in practice.

Medical services and *humanitarian activities* are among the most critical. Their reliance on ICTs makes them particularly vulnerable to disruption, which can have immediate and potentially life-threatening consequences.

IHL requires that these services and activities be respected and protected at all times, and that their functioning be facilitated by states and parties to armed conflict. Efforts are also underway to explore how such protection can be made identifiable and visible in the digital environment, including through continued work on a *digital emblem*.

The special protection afforded to objects indispensable to the survival of the civilian population must likewise be upheld against the dangers arising from ICT activities during armed conflict, including with regard to their data and ICT infrastructure essential to their functioning.

At the same time, ICT activities may be used to commit or facilitate serious violations of IHL, including sexual violence and the recruitment or use of children in hostilities. These prohibitions apply regardless of the means used, including ICTs, raising questions as to how they can be effectively addressed in practice.

Information environment as a vector of harm

In today's armed conflict, ICTs are increasingly used to spread information that violates IHL. While information operations are a common feature of warfare, certain content may be spread through ICT activities which incite or encourage violence, spread terror among the civilian population, expose detainees to public curiosity, or undermine trust in medical and humanitarian services (for further detail, see *here*). Emerging technologies, including AI-generated content, further increase the scale and speed of dissemination, amplifying the risk of harm for civilians.

Whether information is spread through ICTs or other means, the applicable legal framework remains the same. Addressing the risks associated with these ICT-enabled activities requires not only compliance with existing legal obligations, but also proactive engagement with relevant actors, including technology companies and the platforms they operate.

Advancing discussions: where the ICT workstream stands and what comes next

Since its launch in September 2024, the Global IHL Initiative has convened three rounds of global consultations. As far as the ICT workstream is concerned, these consultations have brought together states from different regions, as well as international organizations, civil society and technology companies. These discussions have focused on the most pressing humanitarian and legal challenges arising from ICT activities in armed conflict, as outlined above.

Across these exchanges, participants have emphasized the importance of protecting civilian populations and preserving human dignity in contemporary and future conflicts. Two broad elements have emerged. First, existing IHL rules apply in the ICT environment and must be applied in good faith. Second, strengthening protection requires translating these rules into practice in light of technological developments.

Building on these discussions, the workstream co-chairs Ghana, Luxembourg, Mexico, Switzerland and the ICRC published *a first draft outcome document* on 1 April 2026. This marks an important step in an ongoing process aimed at strengthening respect for IHL in the use of ICTs during armed conflict and identifying practical measures to strengthen its implementation. States and other stakeholders will continue to work together to refine this document, including through the next rounds of consultations under the Global IHL Initiative in *May* and June 2026. By the end of this year, the process aims to produce an outcome document that contributes to a shared understanding of how IHL applies and serves as a reference for future implementation.

As technologies continue to evolve, including artificial intelligence and other emerging capabilities, ICT activities are likely to be conducted at greater scale, speed and, in some cases, with increased autonomy. This may amplify risks of indiscriminate effects, incidental civilian harm and cascading impacts across interconnected systems.

While the ICT workstream focuses on current humanitarian and legal challenges related to ICT activities, these broader trends underscore the importance of continued dialogue to ensure that IHL remains capable of addressing new and evolving risks, including in the interaction of other new technologies with ICTs.

Ultimately, protecting civilians requires ensuring that the use of ICTs does not erode the protections afforded by IHL, but that these protections are upheld and made effective in practice.

See also

- Yéelen Marie Geairon, *Deciding under algorithms: artificial intelligence and the protection of civilian infrastructure in armed conflict*, March 12, 2026
- Tilman Rodenhäuser, Laurent Gisel, Marco Roscini, Samit D'Cunha and Anna Rosalie Greipl, *From hackers to tech companies: IHL and the involvement of civilians in ICT activities in armed conflict*, November 4, 2025
- Tilman Rodenhäuser, *International humanitarian law and connectivity disruptions during armed conflict*, July 3, 2025
- Laurent Gisel and Tilman Rodenhäuser, *A steppingstone for more? Progress on the protection of civilian populations from ICT activities during armed conflict*, February 13, 2025

Tags: Civilians, compliance, Cyber and Information Operations, IHL, international humanitarian law, Means and Methods of Warfare, modern warfare, new technologies, protection, Respect for IHL

Why Nordic governments must uphold the global ban on anti-personnel mines

and maintaining family links

14 mins read

Analysis / Conduct of Hostilities / Cyber / IHL / New Technologies / Technology in Humanitarian Action Matt Pollard & Helen Obregón Gieseken

By the end of 2024, the Office of the United Nations High Commissioner for Refugees ...

9 mins read

Analysis / Conduct of Hostilities / Cyber / IHL / New Technologies / Technology in Humanitarian Action

Anders Ladekarl, Eero Rämö, Grete Herlofson & Ulrika Modéer

As security concerns intensify across Europe following the escalation of the international armed conflict between ...