PREVENTING ICT THREATS TO CIVILIAN POPULATIONS IN TIMES OF ARMED CONFLICT: SIX HUMANITARIAN AND LEGAL PRIORITIES

ICRC Working-Paper, July 2026

The rapid digitalization of societies has brought significant social and economic benefits, and enhanced communication. Reflecting this global development, the Common African position has emphasized that information and communication technologies (ICTs) "are an indispensable part of the lives of human beings throughout the world".[1] In countries affected by armed conflict, reliable ICTs are critical, among other things, for civilians to access essential goods and services, governments to provide such services, and humanitarian organizations to conduct their activities.

Today, the use of ICTs by States and non-State actors poses new threats to civilian populations during armed conflict. Military ICT capabilities offer belligerents the possibility of achieving their objectives without necessarily causing harm to civilians or physical damage to civilian infrastructure; but ICT activities are also frequently used to harm civilian populations, data and infrastructure, and can have significant unintended and incidental effects.

In this working paper, the International Committee of the Red Cross (ICRC) would like to bring to the attention of States six ICT threats for civilian populations that it sees in contemporary armed conflicts. The working paper also suggests proposals for how States could address them in the United Nations Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs (Global Mechanism).

The ICRC recommends that States in the Global Mechanism build on the significant progress made in the recent past to find common understanding on the human cost and legal limits of ICT activities in the context of armed conflicts. This progress includes, in particular, the adoption of a resolution – "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" – at the 34th International Conference of the Red Cross and Red Crescent,[2] and a forthcoming outcome document – *Upholding International Humanitarian Law in the Use of Information and Communication Technologies during Armed Conflicts* – under the Global Initiative to Galvanize Political Commitment to International Humanitarian Law.[3]

[1] African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, 2024.
[2] 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024, *Protecting Civilians and other Protected Persons and Objects Against the Potential Human Cost of ICT Activities during Armed Conflict*, 34IC/24/R2, 2024.
[3] https://www.upholdhumanityinwar.org/en.

1. ICT OPERATIONS DISABLING THE PROVISION OF ESSENTIAL SERVICES

In recent armed conflicts, the ICRC has observed a range of ICT operations that have disabled the provision of essential services for civilian populations. ICT operations against energy infrastructure have resulted in power outages for hundreds of thousands of people; ICT operations against communication infrastructure have prevented people from receiving life-saving information and from maintaining contact with their loved ones; and ICT operations have disrupted transport systems, banking and water supply, and have targeted food production and storage facilities. In countries affected by armed conflict, ICT operations targeting such essential services exacerbate the hardship of civilian populations. In addition, in times of armed conflict there is a heightened threat of ICT and kinetic attacks against the technical infrastructure essential to the general availability and integrity of the internet, including undersea cables, orbit communication networks and data centres.

In countries affected by armed conflict, ICT operations have also disrupted or disabled government services (such as the IT infrastructure of government administrations; courts; border controls; e-services) and private businesses, causing significant economic and social harm.

States have recognized in the Open-Ended Working Group that ICT operations can have "potentially devastating humanitarian consequences".[4] In fact, ICT operations can disable or physically damage civilian critical infrastructure, directly or indirectly causing injury or death to civilians. ICT operations that result in physical damage have received attention; but the use of ICTs in armed conflicts has shown that even in the absence of physical damage, ICT operations can severely disable civilian infrastructure, damage or delete civilian data, and disrupt the delivery of essential services, with significant consequences for civilian populations. In fact, these effects of ICT operations constitute one of the most important ICT threats for civilians.

The ICRC calls on Member States of the Global Mechanism to:

- reaffirm that IHL applies to the use of ICTs in situations of armed conflict, build on the shared understandings developed among States in this regard,[5] and deepen intergovernmental exchanges on the limits that IHL imposes on ICT activities that result in non-physical damage or destruction
- identify practical measures for States to take to build resilience against the harm that ICTs may cause to civilian populations in times of armed conflict, and help build capacity to implement such measures globally.

[4] *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816, 2021, para. 18.

[5] These include, in particular, *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); 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024, *Protecting Civilians and other Protected Persons and Objects Against the Potential Human Cost of ICT Activities during Armed Conflict*, 34IC/24/R2, 2024; *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, Final Report*, A/AC.292/2025/CRP.1, 2025, para. 40(b). Furthermore, the forthcoming outcome document on "Upholding International Humanitarian Law in the Use of Information and Communication Technologies during Armed Conflicts" of the Global Initiative to Galvanize Political Commitment to International Humanitarian Law, which draws on consultations with over 100 States and other stakeholders, provides guidance to facilitate the implementation of IHL obligations relevant to ICT activities during armed conflict in a manner consistent with the protective purpose of IHL.

2. ICT OPERATIONS TARGETING MEDICAL FACILITIES AND HUMANITARIAN ORGANIZATIONS

The ICRC has been voicing concern for years about ICT operations targeting medical facilities. These can have particularly serious consequences in times of armed conflict. Recent years have seen a significant number of ICT operations targeting hospitals and other medical facilities. Accordingly, States have underscored the vulnerability of the health-care sector to malicious ICT activities, expressed concern about them,[6] and have called for "parties to armed conflicts to respect and protect medical personnel, units and transports in accordance with their international legal obligations, including with regard to ICT activities".[7]

Humanitarian organizations, too, are frequently targeted or affected by malicious ICT activities. These activities include distributed-denial-of-service operations, intrusion of systems and exfiltration of sensitive data, and disabling computer systems to disrupt humanitarian operations. In 2022, the ICRC was the victim of an ICT operation that enabled unauthorized access to personal data such as the names, location and contact information of missing people and their families, unaccompanied or separated children, detainees and other people receiving humanitarian services. More recently, the self-registration application of the World Food Programme Palestine suffered a data breach. Such operations do various types of harm to the targeted organizations and, most importantly, compromise the safety and dignity of the people they serve.

As the UN Security Council emphasized, and as States have recalled repeatedly, ICT activities against humanitarian organizations "disrupt their relief operations, undermine trust in humanitarian organizations … and threaten the safety and security of their personnel, premises and assets, and ultimately their access and ability to carry out humanitarian activities".[8]

The ICRC calls on Member States of the Global Mechanism to:

- recall and reaffirm their commitment to the rules of international law, in particular IHL, that require respect and protection for medical units, transports and personnel, as well as humanitarian activities, objects and personnel[9]
- identify and adopt legal and practical measures for States to take to prevent ICT operations that harm medical facilities and humanitarian organizations.

---

[6] *Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 2021, para. 10; *Annual Progress Report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, A/AC.292/2024/CRP.1, 2024, para. 14.

[7] 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024, *Protecting Civilians and other Protected Persons and Objects Against the Potential Human Cost of ICT Activities during Armed Conflict*, 34IC/24/R2, 2024, para. 6.

[8] UNSC, *Resolution 2730*, S/RES/2730, 24 May 2024. See also 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024, *Protecting Civilians and other Protected Persons and Objects Against the Potential Human Cost of ICT Activities during Armed Conflict*, 34IC/24/R2, 2024; *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, Final Report*, A/AC.292/2025/CRP.1, 2025, para. 21.

[9] On the IHL rules that protect impartial humanitarian organizations against ICT activities, see ICRC, *Cyber Operations During Armed Conflict: Protection of Humanitarian Personnel and Objects During Armed Conflict*, 2025.

3. THE USE OF ICTS IN THE RECRUITMENT AND USE OF CHILDREN IN HOSTILITIES

International law sets strict limits on the recruitment and use of children in hostilities.[10] The use of ICTs is, however, transforming the ways that parties to armed conflict and other actors can violate these rules. For instance, in recent armed conflicts, parties have used social media and messaging apps to recruit children into their armed forces or use them in hostilities. The use of ICTs has facilitated the participation of children in hostilities because they no longer need to be physically close to an armed force or armed group: children with smartphones are capable of taking part in cyber operations. It has also extended the reach of recruiters, who can now contact more children more quickly via online communities.

Both the participation of children in hostilities and their recruitment into armed forces or armed groups are unlawful and have harmful consequences for children. Children may not fully understand the risks or legal consequences of their engagement with warring parties. Online recruitment and ICT-facilitated use in hostilities put children at risk of direct attack, arrest for their involvement and other kinds of harm.

The ICRC calls on Member States of the Global Mechanism to:

- recall and reaffirm the rules of international law that prohibit recruitment and use of children in hostilities, and build common understandings of the specific limits they impose in the ICT environment
- identify and adopt legal and practical measures for States to take to prevent child recruitment and use in hostilities, in particular by equipping children and their caregivers with the knowledge and resources to recognize and resist online recruitment and use of children in hostilities.

4. ICT THREATS POSED BY CIVILIAN HACKERS IN ARMED CONFLICTS

The ICRC has observed a sharp rise in the number of civilian hackers ('hacktivists', cyber criminals, non-State actors) – individuals or groups whose conduct is not attributable to a State – conducting ICT activities during armed conflicts. Threat intelligence experts have counted dozens of such hacker groups taking part in inter-State conflicts since 2022, and States warn that some of these non-State actors "have demonstrated ICT capabilities previously only available to States".[11]

Many civilian hackers do not know, or ignore, the limits that IHL imposes on ICT operations. Some of these actors have directed their operations against civilian infrastructure and services, such as medical facilities, food production, civilian transport infrastructure, civilian government services and private businesses.

Civilian hackers, too, must comply with relevant rules of IHL when conducting ICT operations in the context of and in association with an armed conflict.[12] As the Office of the Prosecutor of the

[10] Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict (2000); Additional Protocol I, Article 77(2); Additional Protocol II, Article 4(3)(c); ICRC Customary IHL Study, Rules 136 and 137. See also African Charter on the Rights and Welfare of the Child, Article 22.

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

[12] For an overview of the most relevant IHL rules in this context, see ICRC, *Eight rules for "civilian hackers" during war, and four obligations for states to restrain them*, 2023.

International Criminal Court has said, "any person may be the perpetrator of a cyber-enabled war crime, irrespective of whether they act on behalf of a party to the armed conflict".[13]

The ICRC calls on Member States of the Global Mechanism to:

- recall and reaffirm States' obligation to take all appropriate measures to prevent civilian hackers on the State's territory or under its jurisdiction or control from committing IHL violations through ICT activities, and to suppress such violations if they do occur
- identify and adopt legal and practical measures for States to take to fulfil these obligations and prevent harm caused by these non-State actors.

5. DANGER FOR CIVILIAN POPULATIONS WHEN TECHNOLOGY COMPANIES PROVIDE PRODUCTS AND SERVICES TO PARTIES TO ARMED CONFLICT

Technology companies operate and maintain much of the world's ICT infrastructure (such as communication infrastructure or data centres), and provide their services to a variety of clients, including the armed forces of parties to armed conflict. Recent armed conflicts have shown that when civilian technology companies provide products and services to armed forces, there is a real risk of their assets, infrastructure and employees being regarded as a military objective under IHL. Attacks on the ICT infrastructure provided by technology companies will have wide-ranging effects on civilian populations, which depend on such infrastructure and services in their daily lives.

Under IHL, technology company infrastructure and employees are civilian and therefore protected against attack. However, the protection of civilians may be lost if the company's personnel carry out activities that amount to direct participation in hostilities, or if the company's infrastructure qualifies as a military objective, this infrastructure, too, loses its protection. In all cases, company staff must respect relevant rules of IHL when operating in the context of armed conflict.

Even if a specific piece of infrastructure, or parts thereof, qualify as a military objective, the IHL principles and rules of proportionality and precautions in attack must be respected.[14] They require assessing all reasonably foreseeable direct and indirect effects on civilians and civilian objects, such as harm to civilian populations reliant on the infrastructure for the functioning of essential services; taking all feasible precautions to avoid and at least minimize this harm; and refraining from carrying out the attack if this harm may be expected to be excessive compared to the direct and concrete military advantage anticipated.

The ICRC calls on Member States of the Global Mechanism to:

- build a common understanding of the risks that the military use of ICT infrastructure and services provided by technology companies during armed conflict entails, in particular for a company's civilian personnel and infrastructure, and for civilians relying on their products and services, and recall and reaffirm the IHL rules and principles of distinction, proportionality and precautions in attack that aim to prevent or mitigate civilian harm

[13] International Criminal Court, Office of the Prosecutor, *Policy on Cyber-Enabled Crimes under the Rome Statute*, 2025, para. 81.

[14] On the IHL principles of distinction and proportionality, see ICRC, *Cyber Operations During Armed Conflict: The Principle of Distinction*, 2023; ICRC, *Cyber Operations During Armed Conflict: The Principle of Proportionality*, 2023.

- identify and adopt legal and practical measures for States to take to prevent or mitigate these risks, such as – to the extent feasible – physically or technically separating the infrastructure, services and products used in military operations from those used for civilian purposes.

6. THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN ICT OPERATIONS DURING ARMED CONFLICT

Technological advances in the field of AI have resulted in some AI tools becoming capable of performing complex tasks spanning across the cyber kill chain, from reconnaissance and vulnerability discovery to exploitation and creation of effects. Consequently, State ICT operators are integrating AI into their ICT operations, including in times or armed conflict. Civilian hackers are doing so as well.

The use of AI in ICT activities may increase their speed, scale and potential for harm, including by enabling more rapid identification and exploitation of vulnerabilities and greater autonomy in the conduct of harmful activities. The ICRC is concerned that in situations of armed conflict this may heighten the risk of indiscriminate attacks, incidental civilian harm, damage to critical civilian infrastructure and uncontrolled escalation, particularly in complex and interconnected digital environments.[15] The general availability of advanced AI tools, including some with inadequate 'guardrails' against misuse, increases the risk that these capabilities will expand to or proliferate among actors that are not aware of or disregard the limits that IHL imposes.

The ICRC calls on Member States of the Global Mechanism to:

- recall and reaffirm that ICT operations in armed conflict, including those that involved AI or other emerging technologies, must be conducted in accordance with the existing rules of IHL, and consider whether existing international law provides sufficient safeguards against the harm that increasingly autonomous ICT capabilities can cause, or whether additional limits are needed
- identify and adopt legal and practical measures for States to take – individually and collectively – to prevent risks to civilian populations posed by AI-enabled ICT activities.

[15] See ICRC, *Submission to the United Nations Secretary General on Artificial Intelligence in the Military Domain*, 2024.