ICRC, Protection of civilians against digital threats

The rise of information and communication technologies (ICTs) has reshaped modern armed conflicts, offering strategic advantages while exposing civilians to new and significant risks. Acknowledging these challenges, the ICRC has taken a leading role in examining how International Humanitarian Law applies to cyber operations, providing legal guidance and advocating for stronger protections against digital threats.

Acknowledgments

Case prepared by Agathe de Kerviler, Master student at Paris-Panthéon-Assas University, under the supervision of Louis Perez, doctoral student at Paris-Panthéon-Assas University and Professor Julia Grignon.

A. RESOLUTION ON PROTECTION OF CIVILIANS AGAINST DIGITAL THREATS DURING ARMED CONFLICTS

> [Source: ICRC, Resolution 2, "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict", 34IC/24/R2, 34th International Conference of the Red Cross and Red Crescent, October 2024, available at https://rcrcconference.org/app/uploads/2024/11/34IC_R2-ICT-EN.pdf]

The 34th International Conference of the Red Cross and Red Crescent (International Conference),

[…]

underlining the importance of connectivity and information and communications technologies (ICTs) for the delivery of a variety of goods and services, including medical services for the civilian population, for humanitarian operations, for civilians to seek and receive information in an accessible format about where to find safety and objects essential for their survival, and for maintaining or restoring family links, including in situations of armed conflict,

recalling that the use of ICTs in future conflicts is becoming more likely, and *noting* that ICTs have already been used in armed conflicts in different regions,

[…]

recalling that the function of the International Conference is to contribute to the respect for and development of IHL,

expressing concern that the malicious use of ICT capabilities by parties to armed conflicts may cause harm to the civilian population and other protected persons and objects, including across international borders, in particular where directed against, or incidentally affecting, ICTs that are part of civilian objects, including objects indispensable to the survival of the civilian population, works and installations containing dangerous forces, or civilian critical infrastructure,

[…]

noting the scale, speed, and reach of the spread of malicious ICT activities, in particular through social media platforms, and *expressing concern* that this may cause, instigate, or amplify harm to the civilian population or other protected persons and objects during armed conflict, including when ICTs are used to recruit children into armed forces,

[…]

recognizing that artificial intelligence and other emerging technologies may provide humanitarian, social, economic or developmental benefits for the civilian population, yet noting with concern that the use of artificial intelligence and other emerging technologies in malicious ICT activities may further increase their scale and speed, as well as the harm they may cause,

noting that ICTs may enable or be used to encourage civilians to conduct or support ICT activities in armed conflict, and *expressing concern* that civilians may not be aware of the risks involved or the legal limits and implications applicable to their conduct,

recalling that private technology companies provide a range of ICT products, services and infrastructure on which civilian populations, governments and humanitarian organizations rely, including during armed conflict,

[…]

recognizing that ICTs are essential for efficient and effective humanitarian operations, and *expressing* deep concern about the impact that malicious ICT activities may have on humanitarian organizations, including data breaches and disinformation that target them, disrupting their relief operations, undermining trust in humanitarian organizations, including Movement components, and threatening the safety and security of their personnel, premises and assets, and ultimately their access and ability to carry out humanitarian activities,

[…]

1. *expresses* the shared commitment of all members of the International Conference 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;

[…]

4. *reiterates* that, in situations of armed conflict, IHL rules and principles […] serve to protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities;

5. *calls on* parties to armed conflicts to protect, consistent with their international legal obligations, civilian critical infrastructure that provides services across several States, including the technical infrastructure essential to the general availability or integrity of the internet, including undersea cables and orbit communication networks;

[…]

7. *calls on* States and parties to armed conflicts to allow and facilitate impartial humanitarian activities during armed conflict, including those that rely on ICTs, and to respect and protect humanitarian personnel and objects in accordance with their international legal obligations, including with regard to ICT activities;

B. REPORT ON DIGITAL THREATS

[Source: ICRC's Global Advisory Board on Digital Threats in Armed Conflicts, Report "Protecting Civilians from Digital Threats During Armed Conflicts: Recommendations to states, belligerents, tech companies, and humanitarian organizations", 12 October 2023, available at https://shop.icrc.org/protecting-civilians-against-digital-threats-during-armed-conflict-recommendations-to-states-belligerents-tech-companies-and-humanitarian-organizations-pdf-en.html]

[1] The digitalization of armed conflict also brings new threats for civilians. […] Over the past decade, state and non-state actors have used digital technology to overcome their adversaries militarily, in support of and alongside kinetic operations. In addition, digital technologies have also been used to disrupt critical civilian infrastructure and services, to incite violence against civilian populations, and to undermine humanitarian relief efforts. The malicious use of digital technologies and the spreading of harmful information is increasingly destabilizing societies and aggravates vulnerabilities among the civilian population.

[…]

[2] During armed conflict, the right of belligerents to use digital means to harm the enemy is not unlimited.

International humanitarian law (IHL) sets out fundamental limits on the conduct of hostilities to protect civilians, infrastructure, and soldiers who no longer participate in hostilities.

[…]

A) Recommendations to Belligerents

Recommendation 1

[3] If belligerents conduct cyber and other digital operations, they must comply with the international legal limits and assess, prevent, or mitigate the harm that their operations may cause to civilians, civilian infrastructure, and other protected persons and objects during armed conflict.

[…]

[4] IHL provides long-standing rules to protect civilians against the dangers arising from military operations: these rules must be effectively applied to cyber and other digital operations related to an armed conflict and enforced. In particular, belligerents must not direct cyber operations against civilians or civilian objects. They must refrain from indiscriminate or disproportionate cyber operations, take constant care to spare civilians and civilian objects, and respect and protect medical facilities, personnel, other critical infrastructure, and humanitarian organizations, including the data they rely on.

Recommendation 2

[5] If belligerents conduct cyber operations, they must put in place procedures and technical measures to prevent or mitigate the impact on civilian populations and societies.

[…]

[6] Belligerents should, at a minimum, apply procedures to verify that their target is a military objective under IHL and assess the risk of civilian harm; select an appropriate and reliable means or method for the operation […]. Belligerents should also apply all feasible measures to prevent or limit the repurposing of tools they use.

Recommendation 3

[7] If belligerents conduct information operations, they must comply with their international legal obligations and should assess, prevent, or mitigate harm that their operations may cause to civilians and other protected persons during armed conflict.

[…]

[8] Belligerents must not conduct information operations designed to instrumentalize civilian populations or to harm people, entities, or activities and operations protected under IHL. This means, for example, that they must refrain from encouraging violations of IHL or any advocacy of hatred that incites discrimination, hostility, and violence against civilians. They should assess, prevent, or mitigate the harm that information operations risk causing – directly or indirectly, intended or unintended – to civilian populations.

[…]

Recommendation 4

[9] Belligerents should refrain from shutting down the civilian population’s access to the internet, which risks having significant impact on civilians and can aggravate rather than combat disinformation. If imperative military necessity justifies disruptions or restrictions, mitigation measures should be taken to ensure that civilians are not affected disproportionately and civilian life is preserved as much as possible.

[10] In times of armed conflict, digital information and communication are essential and at times life-saving for civilians. People – and particularly those who find themselves in a vulnerable situation – rely on digital communications to maintain family contact or seek information on where to find safety or access essential services.

[…]

Recommendation 5

[11] Belligerents should not encourage civilians to take a direct part in hostilities through digital operations. They must consider that if they encourage civilians to take part in digital operations related to an armed conflict, civilians risk losing their legal protection and being targeted.

[12] The more civilians take part in digital operations related to an armed conflict, the more difficult it becomes to distinguish between who is a civilian and who is a combatant. As a result, civilians risk being attacked, and this risk is particularly high when they are physically close to hostilities. […] If civilians conduct digital operations related to an armed conflict, belligerents must take steps to ensure that these civilians are aware of and comply with IHL, and be conscious of the implications of directly participating in hostilities. Belligerents should provide clear warnings, including in digital tools, about the risk of losing protection against attack and advice on practical measures civilians may take to protect themselves.

[…]

Recommendation 6

[13] All belligerents must respect and protect the activities of those who provide essential services for victims of armed conflict, in particular medical personnel and facilities, as well as humanitarian organizations.

[…]

B) Recommendations to States

[…]

Recommendation 9

[14] States must raise awareness of the legal rules on the protection of civilians that apply during armed conflict, especially among private actors, and ensure respect for these rules.

[15] In recent conflicts, a wide range of private actors (including hackers and hacker groups, as well as tech companies) have run cyber and other digital operations related to armed conflicts, at times remotely from the territories of third states. […] States have the primary responsibility to ensure respect for IHL, especially by those operating under their instruction, direction, or control or from their territories, and must hold all those who commit violations of IHL to account.

[…]

C) Recommendations to Tech Companies

Recommendation 15

[16] Digital platforms can play a significant role in facilitating the spread of harmful information and the tech companies that run those platforms can do more to address the problem. They should take additional measures to detect signals and analyse the sources, methods of distribution, and types of harmful information that may exist on their platforms, in particular in relation to situations of armed conflict. Their policies, procedures and practices, including content moderation, should align with IHL and human rights standards.

[…]

D) Recommendations to Humanitarian Organizations

Recommendation 19

[17] Humanitarian organizations should take strong measures to protect the data they collect and process, and they should build resilience to digital threats against their IT systems and operations.

[18] Humanitarian organizations often hold highly sensitive personal information that is necessary for their operations, the breach of which can result in real harm to people. They should therefore include adequate data protection and cyber security measures in their operational planning and practice as the risk of harmful digital operations against them is significant.

[…]

Recommendation 25

[19] Humanitarian organizations should build on lessons from other sectors and partner with public and private institutions to develop innovative solutions that safeguard civilian populations and humanitarian operations against digital threats.

[…]

[20] We welcome and commend the ICRC for its work in research and development on issues such as the proposed creation of a "digital emblem", as well as on data protection by design.

DISCUSSION

I. Applicability of IHL rules regulating the conduct of hostilities to cyber operations

[*N.B. The Tallinn Manual on the International Law Applicable to Cyber Operations is a non-binding document written by an International Group of Experts in 2017, at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.*

For the purposes of this case study, we will examine the rules established by these experts, not as binding legal norms, but as a tool for interpreting IHL rules applicable to cyber operations.]

1. (*Document A, preamble and para 1; Document B, paras 2-4, 14 and 15*)

a. Is International Humanitarian Law (IHL) applicable to cyber operations? (Tallinn Manual 2.0, Rule 80, p. 375) More broadly, is IHL applicable to the use of digital means during armed conflicts?

b. Are cyber operations only risks associated with the use of digital means during armed conflicts? Can they be classified as "attacks" under IHL? (P I, Art. 49 ; Tallinn Manual, Rule 30, p.92) If so, under what circumstances?

II. Distinction

2. (*Document A, paras 1 and 4; Document B, paras 3, 4, 11, 12 and 20*)

a. How does the rule of distinction apply to cyberattacks? (P I, Art. 48; P I, Art. 51; CIHL, Rule 1; CIHL, Rule 7, Tallinn Manual 2.0, Rule 93, p. 420)

b. Why is it becoming increasingly difficult to distinguish between civilians and combatants in cyber operations?

c. Can cyberattacks be considered indiscriminate attacks, prohibited under IHL? (P I, Art. 51(4); P I, Art. 51(5); CIHL, Rule 11, Tallinn Manual 2.0, Rule 111, p. 467)

d. In light of the ICRC's proposal for a digital emblem, how could such a tool help reinforce the protection of medical and humanitarian facilities in cyberspace? What legal and technical challenges could arise when integrating this emblem into the existing IHL framework? (P I, Art. 18(1); P I, Art. 38; CIHL, Rule 30)

3. (*Document A, preamble*; *Document B, paras 11 and 12*)

a. What are the consequences for a civilian who directly participates in hostilities? (P I, Art 51(3); P II, Art. 13(3); CIHL, Rule 6)

b. How does IHL apply to civilians engaging in cyberattacks during armed conflicts? Do they risk losing their protection from direct attacks? (Tallinn Manual 2.0, Rule 97, p. 428)

c. Can parties to the conflict lawfully use digital operations to incite or encourage civilians to take a direct part in hostilities? What are the implications of such actions?

d. What measures must States take to ensure that civilians are informed about the legal risks and implications of participating in cyber operations during armed conflicts? How does this relate to their obligation to disseminate IHL? (P I, Art. 83; P II, Art. 19; CIHL, Rule 144)

III. Proportionality and Internet access

4. (*Document A, preamble, paras 5 and 7; Document B, paras 9 and 10*)

a. Under what conditions can a party to an armed conflict justify shutting down Internet access? How does IHL regulate the proportionality of such a measure? Does IHL apply to such shutting down? If so, does it constitute an attack? If it does or does not, does the proportionality principle apply? If so, how? (P I, Art. 51(5)(b); P I, Art. 57; CIHL, Rule 14)

b. How can an Internet shutdown affect humanitarian operations in a conflict zone? (P I, Art. 70; P II, Art. 18; CIHL, Rule 31)

c. How could an Internet shutdown during an armed conflict affect the protection of civilians by hindering access to critical warnings and safety information? (P I, Art 57(2)(c); CIHL, Rule 20; Tallinn Manual 2.0, Rule 113, p. 470)

5. (*Document A, preamble*; *Document B, paras 3, 4, 10 and 13*)

a. How can cyber operations target objects indispensable to the survival of the civilian population during an armed conflict?

b. Can cyber infrastructures, such as digital platforms for humanitarian aid, be considered ‘objects indispensable to the survival of the civilian population’ under IHL? Is the list of protected goods exhaustive? (P I, Art. 54; P II, Art. 14; CIHL, Rule 54; Tallinn Manual 2.0, Rule 141, p. 531)

6. (*Document A, preamble; Document B, paras 7, 8 and 13)*

a. How does the prohibition of perfidy apply to the use of digital tactics, such as disinformation, during armed conflict? How does it differ from ruses of war? Are both prohibited under IHL? How are they distinguished? (P I, Art. 37; CIHL, Rule 65; Tallinn Manual 2.0, Rules 122–123, pp. 491 and 495)

b. Under what circumstances can a disinformation campaign that impersonates a humanitarian organization to deceive the enemy constitute a violation of IHL? (P I, Art. 37(1)(c); P I, Art. 37(1)(d))

IV. Precautions

7. (*Document B, paras 3, 5, 6, 7 and 8)*

a. How do the rules relating to precautionary measures apply to cyber operations? (P I, Art. 57; P I, Art. 58; CIHL, Rules 15-22)

b. What measures must parties to a conflict implement while conducting cyber operations to minimise the risk of civilian harm?

V. State obligations under IHL and their impact on private actors

8. (*Document A, preamble, para. 4; Document B, paras 14, 15 and 16*)

a. What role do technology companies play in cyber operations during armed conflicts?

b. How does the obligation of States to respect and ensure respect for IHL apply to cyber operations? (GC I-

IV, Art. 1; P I, Art 1(1); CIHL, Rule 144)

c. How can States ensure that private actors, such as technology companies or hacker groups, comply with IHL? How can they contribute to protecting civilians from digital threats during armed conflicts?

d. What recommendations does the ICRC make to States and technology companies in this regard?

VI. Protection of humanitarian workers

9. (*Document A, preamble, paras 7; Document B, paras 13, 17 and 18*)

a. How can ICT activities be misused to hinder humanitarian operations in armed conflict zones?

b. How does IHL protect humanitarian organizations from digital threats? (P I, Art. 70; CIHL, Rule 31; CIHL, Rule 32; Tallinn Manual 2.0, Rule 145, p. 540)

c. How can humanitarian organizations enhance their cybersecurity while maintaining neutrality? What risks could arise from cooperation with States or technology companies in this context?