HUMANITARIAN LAW & POLICY

Protecting civilians against digital threats: four worrying trends and recommendations to address them

October 19, 2023, Analysis / New Technologies

11 mins read

Cordula Droege
Chief Legal Officer/Legal Division Head, ICRC

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

Tilman Rodenhäuser
Thematic Legal Adviser, ICRC

Joelle Rizk
Digital Risks Adviser, ICRC

In situations of armed conflict, access to digital technology can save lives. But the use of cyber, information, and other digital operations by belligerents during armed conflict also brings new threats and risks for civilians. Think about cyber operations disrupting civilian infrastructure and services, information operations inciting violence against civilian populations, and digital operations undermining humanitarian relief efforts. In ever-more interdependent digital and physical environments, civilians and civilian infrastructure are increasingly drawn upon to support military operations and, as a result, face real risks of being targeted. As digital technologies permeate our lives and societies, cyber and information operations are no longer abstract or "only online". They can, directly or indirectly, have serious online and 'offline' consequences and harm people.

Between 2021 and 2023, the International Committee of the Red Cross' (ICRC) President convened a Global Advisory Board of high-level experts from the legal, military, policy, technological, and security fields to advise the organization on digital threats and to develop concrete recommendations to protect civilians against such threats. Today, this Board released its report entitled 'Protecting Civilians against Digital Threats During Armed Conflict'. In this post, Cordula Droege (chief legal *officer and head of the legal division of the ICRC), Laurent Gisel (Head of the Arms and Conduct of Hostilities Unit of the ICRC), Tilman Rodenhäuser (Legal Adviser at the ICRC) and Joelle Rizk (Digital Risks Adviser at the ICRC) present four worrying trends the Board identified, and examples of the Board's recommendations to address one of them, namely the growing civilian involvement in digital military operations.*

ICRC Humanitarian Law & Policy Blog · Protecting civilians against digital threats: 4 worrying trends and recommendations to address them

Each new conflict presents new ways in which belligerents and civilians use digital technologies. In this fast-evolving digital environment, threats to civilian populations are rising, boundaries are shifting, and operations are more and more connected. As military operations increasingly rely on digital technology, there are at least four trends that risk putting civilians in harm's way.

One, the more our daily lives rely on digital infrastructure, services, and data, the greater the risk that cyber operations during armed conflict harm civilians by disrupting infrastructure, services, and data essential to human safety and dignity and the functioning of society. Cyber operations have the potential to disable or physically damage industrial facilities, communication networks, and other elements of a state's critical civilian infrastructure in ways that could directly or indirectly cause harm, injury, or death to civilians, including by preventing the proper functioning of essential services and the delivery of humanitarian relief.

Two, while the use of connectivity and digital tools is often essential for civilians to access life-saving information in times of armed conflict, the latter can also amplify harmful information. Information operations have long been part of armed conflicts. Today, however, harmful digital information occurs at greater scale, speed, and reach than ever before. Harmful information spreads across multiple information ecosystems and platforms, distorting facts, influencing people's beliefs and behaviours, raising tensions, triggering violence against civilians and their properties as well as displacement, fostering distrust and spreading hatred online and offline.

Three, cyber operations, data breaches, and disinformation can undermine the trust in humanitarian organizations and their ability to provide life-saving services to people affected by armed conflict. In a global context marked by staggering needs and an insufficient humanitarian response capacity, digital threats can weaken humanitarian operations and organizations. Threats are multi-faceted. They include cyber operations that risk disrupting or destroying humanitarian organizations' digital infrastructure and communication, or penetrating their systems to exfiltrate data. They also include disinformation aimed at jeopardizing humanitarian organizations' reputation and undermining their ability to operate.

Four, with the digitalization of societies, there are fundamental shifts in the types of behaviors of civilians during armed conflict and their possible involvement in digital military operations – on their own volition or encouraged by warring parties. For example, civilian hackers have conducted a myriad of cyber operations in relation to armed conflicts; tech companies provide various services not only to civilian populations in conflict-affected areas, but also to armed forces; and digital tools are used to encourage or nudge civilians to collect militarily-relevant information. In light of these developments, in practice the fundamental distinction between what is civilian and what is military risks becoming blurred – putting civilians and civilian infrastructure at higher risk of attacks, retaliation or other harmful acts.

A call to global action: recommendations by the Global Advisory Board

Drawing on the diverse professional backgrounds and experience of its members, the Global Advisory Board calls for the protection of civilians from digital threats, and respect for international humanitarian law, to become a global strategic priority for the international community. To reduce the risk of harm, the Board developed a set of concrete recommendations for belligerents (be they state or non-state actors), states, tech companies, and humanitarian organizations to prevent or mitigate digital threats to civilians during armed conflict. These recommendations are based on four overarching principles, namely:

- Digital space is not a lawless space, including during armed conflict;
- Protecting civilians from digital threats requires investment in legislation, policies, and procedures;
- Political and military leaders should make the protection of civilians against digital threats a priority in ongoing and future armed conflicts; and
- States, tech companies, humanitarian organizations, civil society, and other stakeholders should join forces to use digital technology to enhance the protection of civilians.

As this post cannot present these principles and recommendations in their entirety, it focuses on those related to the fourth trend described above, namely the risk of civilians being drawn into military operations.

Addressing multiple risks when civilians are drawn into digital military operations

Military, political, and tech decision-makers must be aware that 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. The closer digital technologies draw civilians to hostilities, the greater the risk of harm. And the more digital infrastructure or services are shared between civilians and militaries, the greater the risk of that infrastructure being attacked. With a view to protecting civilians and civilian infrastructure against harm, belligerents, States, tech companies and humanitarian organizations should take effective preventive and mitigating measures. The ICRC Global Advisory Board offers the following multidisciplinary and interconnected recommendations.

In situations of armed conflict, belligerents – state and non-state – "should not encourage civilians to take a direct part in hostilities though 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." The Board calls on belligerents to ensure that when civilians are involved in digital operations related to an armed conflict, these civilians are aware of and comply with IHL, and be conscious of the implications of directly participating in hostilities, or being (mis)perceived to do so. Belligerents should provide clear warnings, including in the design of digital tools, about the risk of losing protection against attack and advice on practical measures civilians may take to protect themselves.

Turning to the specific responsibilities of states in this respect, the Board offers three recommendations:

First, "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." This recommendation recalls existing international humanitarian law obligations.

Second, to prevent harm to civilians, the Board calls on states "to regulate the growing market of tech companies that develop and sell capabilities and services developed with the objective of harming civilians". In other words, the Board recommends that states take measures to ensure that tech companies do not provide tools or services designed for digital operations that would violate international humanitarian law.

Third, the Board emphasized that "states should, to the maximum extent feasible, segment data and communications infrastructure used for military purposes from civilian ones." The Board notes that digital military operations will in most cases use some of the internet's civilian infrastructure, networks, and platforms. Yet, to protect civilian infrastructure and data from attack, it recommends that as a default position, states should, whenever feasible, attempt to segment – namely physically or technically separate – digital infrastructure (or parts thereof) that are used for military purposes from civilian ones. For example, when deciding whether to store military data on a non-segmented commercial cloud predominantly used for civilian purposes, a segment of such a commercial cloud, or on dedicated military infrastructure, military planners and operators should avoid using the non-segmented commercial cloud.

This last issue is also reflected in the recommendations to tech companies, who "should, to the maximum extent feasible, segment data and communications infrastructure they provide for military purposes from civilian ones." Said differently, if offering infrastructure for use by the military, tech companies should, whenever possible, offer digital infrastructure (or parts thereof) that is segmented from that used by civilians, as a means of protecting civilian infrastructure and data from attack and from incidental harm.

Finally, and in recognition of the multiplicity of stakeholders needed to effectively address current threats and to protect civilians, the Board recommends that "humanitarian organizations with relevant expertise and capacity should strengthen their efforts to raise awareness of the legal rules on the protection of civilians that apply during armed conflict, including among private actors conducting digital operations." The Board elaborates that humanitarian organizations should raise awareness of IHL among private actors, for instance through public communication, IHL-compliant model codes of conduct, videos or apps educating such actors about the applicable rules, and engaging hacker groups to respect IHL rules when applicable. The ICRC's recent publication of '*8 Rules for Civilian Hackers during War and 4 Obligations for States to Restrain Them*', is a direct and concrete effort to give effect to this recommendation. Moreover, the Board proposes that humanitarian organizations, states, and tech companies seek partnerships with engineering schools to make future operators aware of the specific rules applicable when conducting cyber, *information*, or other digital operations during armed conflict and the associated risks.

***

The use of digital technologies during armed conflict is only likely to grow. The Global Advisory Board calls on the international community and all relevant stakeholders to join forces and work in an open and inclusive manner to protect civilians against digital threats during armed conflicts. Every sector has an important role to play. The Board emphasizes that the protection of civilians must be based on international humanitarian law, but also cautions that 'these long-standing rules need to be interpreted and applied in ways that ensure adequate protection for civilians, civilian infrastructure, data, and other protected objects in our ever-increasingly digitalized societies'. The Board's truly international and multistakeholder recommendations will hopefully help inform and guide action to this effect.

See also

- ICRC position paper, *International humanitarian law and cyber operations during armed conflicts*, November 28, 2019
- Tilman Rodenhäuser & Samit D'Cunha, *Foghorns of war: IHL and information operations during armed conflict*, October 12, 2023
- Tilman Rodenhäuser & Mauro Vignati, *8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them*, October 4, 2023
- Joelle Rizk & Sean Cordey, *What we don't understand about digital risks in armed conflict and what to do about it*, July 27, 2023
- Pierrick Devidal, *'Back to basics' with a digital twist: humanitarian principles and dilemmas in the digital age*, February 2, 2023
- Tilman Rodenhäuser, Balthasar Staehelin & Massimo Marelli, *Safeguarding humanitarian organizations from digital threats*, October 13, 2022

Tags: cybersecurity, digital age, Global Advisory Board, ICRC, protection of civilians

You may also be interested in:

ICRC engagement with armed groups in 2023

🕓 12 mins read

Analysis / New Technologies Matthew Bamber-Zryd

In line with its mandate, the ICRC engages with all parties to an armed conflict, including non-state armed groups. The ICRC has a …

Space security governance: steps to limit the human costs of military operations in outer space

🕓 13 mins read

Analysis / New Technologies Nivedita Raju

Civilians are heavily dependent on space systems for everyday life. Yet, those same space systems can also be critical for national and international …