PROTECTING CIVILIANS AGAINST DIGITAL THREATS DURING ARMED CONFLICT

RECOMMENDATIONS TO STATES, BELLIGERENTS, TECH COMPANIES, AND HUMANITARIAN ORGANIZATIONS

FINAL REPORT OF THE ICRC GLOBAL ADVISORY BOARD ON DIGITAL THREATS DURING ARMED CONFLICTS

EXECUTIVE SUMMARY
PROTECTING CIVILIANS AGAINST DIGITAL THREATS DURING ARMED CONFLICT
RECOMMENDATIONS TO STATES, BELLIGERENTS, TECH COMPANIES, AND HUMANITARIAN ORGANIZATIONS

FINAL REPORT OF THE ICRC GLOBAL ADVISORY BOARD ON DIGITAL THREATS DURING ARMED CONFLICTS

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Between 2021 and 2023, the International Committee of the Red Cross (ICRC) convened a global advisory board of high-level leaders and 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. This report presents a set of concrete recommendations to belligerents, states, tech companies, and humanitarian organizations to prevent or mitigate digital threats to civilian populations.

FOUR GUIDING PRINCIPLES THAT UNDERLIE THE BOARD’S RECOMMENDATIONS

I. Digital space is not a lawless space, including during armed conflict. States, belligerents and everyone who conducts digital operations related to an armed conflict must respect the international legal limits, in particular international humanitarian law (IHL). 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. Common understandings, or guidelines, to clarify the interpretation of IHL in digital contexts would reduce ambiguity and prevent harm.

II. Protecting civilians from digital threats requires investment in legislation, policies, and procedures. Such action should be taken by states and societies to build resilience against digital threats by states and companies that build and frame the digital environment, and by those conducting digital operations. We cannot allow the digitalization of armed conflict to jeopardize the protection of civilians. The fact that adopting and implementing such legislation, policies, and procedures may be politically, commercially, or technically complicated is no excuse for not implementing them.

III. Political and military leaders should focus on protecting civilians. They should 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. In practice, this means that there is a growing risk of civilians and civilian infrastructure being targeted during armed conflict.

IV. States, tech companies, humanitarian organizations, civil society, and other stakeholders should join forces to use digital technology to enhance the protection of civilians. Collectively, we should harness the potential of digital technologies to protect civilians from harm, to enable and empower civilians to address their needs during conflict, and to facilitate more effective and efficient humanitarian services.
THE BOARD’S RECOMMENDATIONS TO BELLIGERENTS

**Recommendation 1:** 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.

**Recommendation 2:** 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.

**Recommendation 3:** 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.

**Recommendation 4:** 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.

**Recommendation 5:** 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.

**Recommendation 6:** 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. States should reaffirm – online and offline – this long-standing consensus.

THE BOARD’S RECOMMENDATIONS TO STATES

**Recommendation 7:** States and societies should build resilience against digital disruption by strengthening the cyber security of civilian infrastructure, services, and data, and by developing contingency plans.

**Recommendation 8:** States and societies should build resilience against harmful information, uphold the right to freedom of expression, and protect journalists.

**Recommendation 9:** 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.

**Recommendation 10:** If new legal rules and norms are developed, they need to build upon and strengthen – not undermine – the protection of civilians and other protected persons and objects that existing international legal rules provide.

**Recommendation 11:** States should, to the maximum extent feasible, segment data and communications infrastructure used for military purposes from civilian ones.

**Recommendation 12:** To prevent harm to civilians, states need to regulate the growing market of tech companies that develop and sell capabilities and services developed with the objective of harming civilians.

**Recommendation 13:** If states or international organizations restrict the export or import of information and communication technologies (ICTs) through sanctions or other restrictive measures towards countries affected by armed conflict or other humanitarian crises, specific humanitarian exemptions for ICT equipment and services are necessary to ensure the operation, functioning, maintenance, and safety of medical services, and the timely delivery of humanitarian activities or other services essential to meet the basic needs of civilian populations.

**Recommendation 14:** States and other actors should support and facilitate the development of adequate cyber security and data protection measures and policies for humanitarian organizations, and provide support to bolster the ability of those organizations to respond to harmful information.
THE BOARD’S RECOMMENDATIONS TO TECH COMPANIES

**Recommendation 15:** 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.

**Recommendation 16:** Tech companies that operate in situations of armed conflict should understand and monitor whether the services they provide may amount to a direct participation in hostilities by their employees and whether the company might qualify as a military objective; and understand and monitor whether beyond direct participation in hostilities, their involvement in armed conflict situations might put their employees at risk, and if necessary, adjust their activities accordingly.

**Recommendation 17:** Tech companies should, to the maximum extent feasible, segment data and communications infrastructure they provide for military purposes from civilian ones.

**Recommendation 18:** Tech companies should ensure that measures they take voluntarily for commercial or other reasons – meaning outside their legal obligations, such as those imposed by sanctions and other restrictive measures – do not impede the functioning, maintenance, and safety of medical services, humanitarian activities, or other services essential to meet the basic needs of civilian populations.

THE BOARD’S RECOMMENDATIONS TO HUMANITARIAN ORGANIZATIONS

**Recommendation 19:** 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.

**Recommendation 20:** Humanitarian organizations should prepare to be the target of harmful information that may affect their operations and reputation, and be prepared to respond appropriately, both online and offline.

**Recommendation 21:** Humanitarian organizations should develop responses to harmful information against civilians in their operations.

**Recommendation 22:** 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’S RECOMMENDATIONS ON WORKING TOGETHER

**Recommendation 23:** Multistakeholder dialogue is needed to bring together expertise of states, tech companies, humanitarian organizations, international organizations, academia, civil society and other stakeholders to develop conflict-specific understanding, principles, and/or guidelines to protect civilians against digital threats.

**Recommendation 24:** Tech companies and humanitarian organizations should work together to address digital threats during armed conflict.

**Recommendation 25:** 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.
MISSION
The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.