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
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
CONTENTS

Executive Summary.................................................................................................................. 3

Introduction................................................................................................................................. 6

Civilians Under Threat: Four Worrying Trends in an Interconnected and Evolving Digital Environment During Armed Conflict........................................................................................................ 7

A Call to Global Action: Recommendations by the Global Advisory Board ................................ 9
  Recommendations to Belligerents .......................................................................................... 10
  Recommendations to States................................................................................................. 11
  Recommendations to Tech Companies............................................................................... 14
  Recommendations to Humanitarian Organizations .......................................................... 15
  Working Together................................................................................................................ 17

The Way Forward ...................................................................................................................... 18

Members of the ICRC’s Global Advisory Board on Digital Threats During Armed Conflicts........ 19

Definitions and Concepts ......................................................................................................... 20
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.
INTRODUCTION

In situations of armed conflict, access to digital technology can save lives. For example, it enables people to seek information about where to find safety, allows them to contact and find family members they lost contact with, permits medical facilities to function, and is used by humanitarian organizations and governments to assist people as effectively as possible.

The digitalization of armed conflict also brings new threats for civilians. While the armed conflict in Ukraine has focused the world’s attention on the issue, we have long observed digital threats in other conflicts and humanitarian crises. What we observe today is likely foreshadowing the future: digital threats will become a growing concern 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. In ever-more interdependent digital and physical environments, civilians and civilian infrastructure are not only in the crosshairs of hostile operations but also increasingly drawn upon to support military operations. As digital technologies permeate our lives and societies, cyber and information operations are no longer abstract or “only online” but harm people.

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. We, the International Committee of the Red Cross (ICRC) Global Advisory Board on Digital Threats During Armed Conflicts, have based our work on the international consensus that the established principles and rules of IHL apply to all forms of warfare and to all kinds of weapons, be they new or old, digital or physical.

Addressing digital threats becomes ever-more complex. New questions and dilemmas emerge. How can societies protect themselves against cyber operations that disrupt the functionality of essential civilian services and infrastructure? How is personal and humanitarian data protected against damage, destruction, misappropriation, and non-consensual publication? What limits exist – or should exist – for information operations? What role do and should tech companies play in protecting civilian populations? What risks arise if civilians and tech companies become increasingly involved in armed conflicts through digital means, and if civilian digital infrastructure is used for military operations? How do we safeguard in the digital age the long-standing consensus that those who work to assist victims of armed conflict must be protected against harm?

To prevent or mitigate harm to civilians, the time to act is now. In pursuance of its humanitarian mission to protect the lives and dignity of victims of armed conflict, the ICRC convened this board of high-level leaders and experts from the legal, military, policy, technological, and security fields. Between 2021 and 2023, the board advised the ICRC on digital threats and how to position itself in this respect, and identified concrete recommendations to protect civilians against digital threats. With its expertise and focus on armed conflict, the board hopes to contribute to the important debate on preserving a human-centred approach to new technologies, as well as the advancement of international law in new contexts.

This report presents four guiding principles and a set of concrete recommendations to belligerents, states, tech companies, and humanitarian organizations to prevent or mitigate digital threats to civilian populations. It reflects a consensus among the members of the board; it does not necessarily reflect the views of organizations, institutions, or companies that members are affiliated with.
From the growing use of artificial intelligence in cyber and information operations that increases their speed and reach, to ever-more intrusive surveillance practices, digital innovation is used in many ways during armed conflict. 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 increasingly connected. For instance, cyber operations are conducted to support information and kinetic operations, such as to prevent the target from using communication channels to counter hostile operations, or to increase their impact. Similarly, information operations are conducted to reinforce and enhance the disruptive effect of cyber operations. Artificial intelligence is used in cyber offence as well as defence operations, and to create content used in information operations.

In the light of this fast-paced development of military innovation and the use of digital technologies to overcome an adversary, we are concerned that digitalizing warfare is inflicting additional harm on people.

1. **Cyber Operations during Armed Conflict Risk Harming Civilians by Disrupting Infrastructure, Services, and Data Essential to Human Safety and Dignity and the Functioning of Society.**

The more our daily lives rely on digital infrastructure, services, and data, the greater the risk that the use of cyber operations during an armed conflict will cause harm to civilian populations. Cyber operations have the potential to disable or physically damage industrial facilities, communication networks, and other elements of a state’s critical 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. Cyber operations designed to manipulate information for cognitive and psychological effects could have similar consequences, including through the stealing, leaking, manipulating, or deleting of data. Due to the interconnectivity that characterizes cyberspace, there is a real risk that cyber operations will – if designed to do so or if not properly tested or controlled – indiscriminately affect widely used computer systems and connected civilian infrastructure far beyond the theatre of conflict, directly or indirectly causing damage, injury, or death to civilians, and further escalating conflicts.

2. **The Use of Connectivity and Digital Tools is Essential for Civilians to Access Life-Saving Information in Times of Armed Conflict – But the Latter Can Also Amplify Harmful Information.**

Information operations have long been part of armed conflict. They are legally permitted in certain circumstances, for instance to warn civilians of military attacks or to deceive the adversary in accordance with international law. Today, digitalization has amplified the scale, speed, and reach of such operations. Overlapping with and at times consisting of disinformation (commonly understood as false or manipulated information intended to cause harm), they spread across multiple platforms, distorting facts, influencing people’s beliefs and behaviours, raising tensions, and increasing the risks of harm to civilians by fostering distrust and spreading hatred online and offline. This can in particular affect women, children, and minorities who find themselves in a vulnerable situation. Furthermore, harmful information negatively affects the availability, integrity, and reliability of critical information that civilians need for their safety and survival in times of conflict. Compared to legacy media, harmful information often spreads more easily on digital platforms and without sufficient editorial oversight. Civilians may unknowingly amplify harmful content.
3. IN THE DIGITAL ENVIRONMENT, DISTINGUISHING WHAT IS CIVILIAN FROM WHAT IS MILITARY RISKS BECOMING BLURRED – AND CIVILIANS AND THEIR INFRASTRUCTURE BECOMING THE TARGET OF ATTACKS.

Civilian actors – people and companies – have long been used to performing military functions during armed conflicts and to assist in the war effort. With the digitalization of societies, we are witnessing fundamental shifts in the types of operations they conduct and the number of civilian actors that involve themselves in armed conflict. At times, this arises from the civilian actors’ own motivation or is based on contracts requiring them to provide cyber security; at times, it is mandated, encouraged, or facilitated by states. This development comes with frequently overlooked risks for civilian populations: the closer digital technologies move civilians to hostilities, the greater the risk of harm they are exposed to. The more digital infrastructure or services are shared between civilians and militaries, the greater the risk of civilian infrastructure being attacked. While IHL is built on the cardinal principle of distinction between what is civilian and what is military, the growing civilian involvement in military operations through digital means, and the use of civilian digital infrastructure for military purposes, risks blurring the lines between the two and thus undermining this fundamental premise.

4. CYBER OPERATIONS, DATA BREACHES, AND DISINFORMATION UNDERMINE THE TRUST IN HUMANITARIAN ORGANIZATIONS AND THEIR ABILITY TO PROVIDE LIFE-SAVING SERVICES TO PEOPLE.

Recent cyber operations and disinformation campaigns against humanitarian organizations – such as against the ICRC in 2022 – should be a wake-up call: in a global context marked by staggering needs and an insufficient humanitarian response capacity, digital threats can weaken humanitarian operations and institutions. They take different forms, from cyber operations disrupting or destroying humanitarian organizations’ digital infrastructure and communication, to operations that penetrate their systems to exfiltrate data, to disinformation operations aimed at jeopardizing humanitarian organizations’ reputation and undermining their ability to operate. Such threats can cause significant harm when they materialize: humanitarian data can be misused to target or persecute civilians receiving humanitarian services, who are often at particular risk. Disrupting humanitarian relief operations, such as their logistics, will likely exacerbate the needs of people affected by conflict and other humanitarian crises. In addition, disinformation and data breaches risk undermining the trust that civilians and parties to armed conflicts place in humanitarian organizations, which affects those organizations’ access to people and can put the safety of their personnel at risk.
A CALL TO GLOBAL ACTION: RECOMMENDATIONS BY THE GLOBAL ADVISORY BOARD

The protection of civilians from digital threats, and fostering respect for IHL, must become a strategic priority. This requires concerted and joined-up efforts from several actors. Drawing on our diverse professional backgrounds and experience, we call on states and other belligerents to reaffirm the existing international legal rules that limit digital operations related to an armed conflict. States, together with civil society and companies, should build a common understanding of existing and possible future limits for digital operations related to an armed conflict.

To prevent or mitigate harm, we have developed four guiding principles and a set of concrete recommendations for belligerents (be they states or private actors), states, tech companies, and humanitarian organizations to prevent or mitigate digital threats to civilians during armed conflict.

FOUR GUIDING PRINCIPLES UNDERLIE OUR 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 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. A common understanding or guidelines that 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.
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.

In times of armed conflict, the responsible behaviour of belligerents in cyberspace must be defined in terms of compliance with international law, at the very least. 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
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.

To ensure that cyber operators prevent or reduce the impact of their operations on civilians, civilian infrastructure, medical facilities, and other protected people and objects, parties to armed conflicts must have clear internal rules and employ rigorous targeting procedures reflecting their international legal obligations. 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; test the means or method prior to employment; apply appropriately fine-grained geographic, temporal, and system “fencing”, a “kill-switch”, and other appropriate techniques and procedures to minimize the risk of incidental civilian harm; continuously monitor, control, and command the operation to prevent unintended consequences; and halt any operation expected not to be consistent with those principles. Belligerents should also apply all feasible measures to prevent or limit the repurposing of tools they use.

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.

In times of armed conflict, several fields of international law impose limits on information operations, in particular IHL and human rights law. 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. At the same time, they must respect and protect freedom of expression and the media and ensure the safety of journalists in order to facilitate access to trustworthy information essential to the safety and dignity of civilians in times of 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.

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. Therefore, shutting the internet down can have a significant impact on civilian populations and should be avoided, in particular if less far-reaching measures are feasible to achieve a military aim. If imperative military necessity justifies disruptions and restrictions, mitigation measures should be taken to ensure the availability of essential services and preserve the life and dignity of civilians 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.

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. Belligerents should therefore reverse the trend of encouraging civilians to take part in digital operations related to an armed conflict, and not provide them with the means to do so. 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. Under IHL, civilians do not lose protection against attack if they are using digital means for any reason other than a direct participation in hostilities, such as in a personal capacity, as journalists, or for documenting crimes.

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 – as much online as offline – this long-standing consensus.

States and other belligerents should explicitly reaffirm – unilaterally, bilaterally, and multilaterally – their commitment to respecting and protecting medical services and impartial humanitarian activities, data, and personnel as much online as offline, and to facilitating their operations in the digital environment. It is important that these protections be reflected in national law and policy and effectively implemented.

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.

States must take all feasible precautions to protect the civilian population against the dangers resulting from digital operations, without undermining their human rights obligations. Around the world, and despite many years of encouragement, there is still insufficient attention paid to implementing even basic cyber security measures. Governments, companies, and non-governmental organizations should be assiduous in working together to, at a minimum, implement the basic cyber security measures that will protect devices, networks, and data from the bulk of cyber threats (sometimes called “cyber hygiene”), including by raising the cyber security awareness and digital literacy of their employees and the general population. To safeguard civilian populations from cyber operations, tech companies should develop their products with “safety by design”. Tech companies have a particular responsibility towards people in conflict zones, of which they should be mindful as they develop software, infrastructure, and services.

But even having done so, states should also expect that some – and in particular the most sophisticated – cyber operations will still produce adverse effects. Therefore, they should build resilience into how they
operate digital services essential for the population. For example, they should take measures to ensure redundancy and to back data up (ideally in geographically and digitally separate locations, such as clouds) and have contingency plans in place to maintain essential services and data for scenarios that include loss of internet access or the deletion of data.

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

To build societal resilience against harmful information, including during armed conflict, a whole-of-society approach is needed to ensure that reliable sources of information are available and known, that journalists and media are protected, and that civilian populations are aware of which information sources they can rely on during emergencies. Building such resilience is a long-term endeavour and needs to commence before any conflict erupts. It also requires states (individually and collectively) to develop appropriate legal and policy frameworks to ensure that the services of tech companies are not misused for violations of international law or to harm civilians in other ways.

States must uphold the right to freedom of expression. During armed conflict, derogations and restrictions of this right must be narrowly construed and comply strictly with the principles of legality, necessity, and proportionality to protect legitimate objectives set out in international human rights law. As there is often no consensus on what is true and what is false, alleged falsity or manipulation of information alone is not a sufficient ground for restricting freedom of expression under international law.

**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.

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. These operations may be defensive and/or offensive in nature. Without regard to IHL, these actors risk further escalating conflicts and tensions.

When conducting such operations, private actors must not target civilians and civilian infrastructure and they may incur international criminal responsibility for certain IHL violations. 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. States should also make private actors aware of the legal and practical risks that participation in hostilities entails. Moreover, states must protect the human rights of everybody under their jurisdiction, including against the digital threats posed by private actors.

**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 for.

States developed IHL primarily with traditional means and methods of warfare in mind. Established international legal rules and principles on the protection of civilian populations and objects apply, however, “to all forms of warfare and kinds of weapons”, including “those of the future”. This encompasses cyber and other digital operations related to an armed conflict.

We call on states to develop a common understanding of how IHL applies to digital operations to ensure adequate protection for civilians, civilian infrastructure (including ICT systems), and data in our ever-

---

1 International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996 (Nuclear Weapons Advisory Opinion)*, para. 86.
increasingly digitalized societies. Possible challenges in applying IHL to the use of digital technology during armed conflict because of the novelty of the technology and its effects cannot be used as a loophole to undermine the protection of civilians. In particular, we urge states to afford civilian data the same IHL protection as civilian objects; it would be unconscionable if digitalizing civilian information and other content would exclude them from existing legal protection.

We do not believe that new rules are needed each time technologies of warfare evolve. However, if it were found that existing international law cannot be interpreted – or is in practice not applied – to ensure the protection of civilians and civilian infrastructure and data against digital operations, additional rules might be needed. If new rules are developed, they need to build upon and strengthen the existing protection of civilians during armed conflict, not undermine it.

We recall that any voluntary, non-binding norms of responsible behaviour in cyberspace agreed in UN processes may sit alongside each other. These norms do not seek to limit or prohibit action that is otherwise consistent with international law and do not undermine the existing legal framework.

**RECOMMENDATION 11**

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

States should be aware that when their military planners and operators use civilian digital infrastructure during armed conflict – such as communication systems or clouds – such civilian infrastructure may turn into a military objective. We note that if the military conducts digital operations, it will in most cases use some of the internet’s ubiquitously used civilian infrastructure, networks, and platforms. However, to protect civilian infrastructure and data from attack, 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, a segment of a commercial cloud or dedicated military infrastructure, military planners and operators should not use the non-segmented commercial cloud. States that use a non-segmented commercial cloud could be regarded as deliberately shielding their own military assets with civilian infrastructure. We reiterate that civilian infrastructure and services must not be attacked.

**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.

Different tech companies offer a range of services to public and private clients. These can include capabilities and services that can be used for digital operations related to an armed conflict and – deliberately or not – result in harm to civilians. States must implement regulations to ensure that tech companies do not develop tools that are inherently unlawful and that companies do not offer services that result in violations of international law. Moreover, states should use existing frameworks, such as export controls, to prohibit companies from selling capabilities and services for digital operations to actors that are likely to use them in violation of international law.

**RECOMMENDATION 13**

If states or international organizations restrict the export or import of 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.

States should build on the United Nations Security Council Resolution 2664, which explicitly excludes from the scope of UN sanctions “the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance or to support other activities that support basic human needs”, whether provided
by the public or private sector. ICT services, hardware and software are often essential for the delivery of medical and humanitarian services to people affected by armed conflict or other humanitarian crises. Imposing restrictions on their import, export, or delivery risks impacting the ability of medical services and humanitarian organizations to operate and undermines their cyber security. For example, if medical facilities cannot update their IT systems, their cyber security is weakened. In addition, having to comply with sanctions and restrictive measures taken by entities associated with or supporting parties to conflict may jeopardize the perception of the impartiality, neutrality, and independence of humanitarian organizations, and ultimately threaten their access and security.

Authorities that impose restrictive measures should consult and coordinate with all concerned actors, in particular tech companies falling within the scope of a restrictive measure, and provide adequate guidance to ensure that those exemptions are effectively implemented in practice.

**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 (see also Recommendation 19 below).

Humanitarian organizations have to build human and technical capacities to effectively protect their operations and the trust people put into them against digital threats within their existing means. A joint effort by states, companies, and other actors is needed to strengthen these organizations’ resilience against digital threats – be it through awareness-raising, funding, services, or the research and development of technological solutions that accommodate humanitarian organizations’ working procedures, in particular the principles of impartiality, neutrality, and independence.

**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.

To address the heightened risk of harmful information spreading in countries affected by armed conflict and other humanitarian crises, tech companies that run digital platforms should implement clear policies on heightened due diligence and enhanced risk management strategies. The UN Guiding Principles on Business and Human Rights and other standards can provide useful guidance in this respect. Tech companies should assess and mitigate any potential negative impacts of their activities on the safety and dignity of people. They should invest adequately and deploy effective measures to limit the emergence and spread of harmful information. Furthermore, tech companies that run digital platforms should review their business practices and ensure that their operations, data collection, and data processing practices do not encourage or facilitate harmful information and are compliant with IHL and human rights standards.

Tech companies that run digital platforms should align their policies, procedures, and practices with IHL and human rights standards. In particular, they should take measures to prevent and address the incitements of IHL violations and dissemination of hate speech that constitutes discrimination, hostility, and violence against civilians or international crimes. While using artificial intelligence can be useful to identify and analyse harmful information, tech companies should ensure that automated procedures include robust human review and steps are taken to reduce biases. They should invest in sufficient expertise in the relevant languages and local contexts, including through collaboration with fact-checking organizations and civil society.
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.

Tech companies provide a range of products and services, for instance communication infrastructure, cloud storage, and cyber security services to defend government and private customers. During armed conflict, companies should inform employees of the risks and legal consequences this may entail. To the extent feasible, companies should also monitor whether belligerents use their civilian services for military purposes and prevent or minimize such use if feasible. They should do everything feasible to minimize the risks to the company and civilian clients that arise in the context of armed conflicts.

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

Tech companies should be aware that digital infrastructure and services – such as communication systems or clouds – may become military targets during armed conflict if used for military purposes. Therefore, if offering infrastructure for use by the military, tech companies should, whenever possible, offer digital infrastructure (or parts thereof) that is segmented (i.e. physically or technically separated) from that used by civilians, as a means of protecting civilian infrastructure and data from attack and from incidental harm.

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.

While tech companies must comply with their legal obligations, such as those imposed by sanctions and other restrictive measures, they should also ensure, to the maximum extent feasible, that measures they take voluntarily and outside their legal obligations do not impede ICT services, hardware, and software for the delivery of medical and humanitarian services to people affected by armed conflict or other humanitarian crises.

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.

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. Building resilience requires making cyber security and data protection an institutional priority and developing internal procedures and structures to prevent harmful digital operations and to minimize the impact when they occur. It also requires investing in technical cyber security measures that are appropriate to the operational context and organization’s mandate; to handle data transparently, accountably, in full respect of the rights and dignity of data subjects, and in line with
international standards; and to continuously train staff. Humanitarian organizations should also take initiative and advocate for strong and clear protection at all times, including for the exclusively humanitarian access to and use of data they collect. The safety, dignity, and resilience of the people they serve is at stake.

**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.

To anticipate and mitigate the threats that harmful information poses to humanitarian organizations, these organizations should build capacity to gather and disseminate accurate information from verified sources, online and offline. This requires ensuring that an organization’s preparedness and contingency planning takes account of their exposure to harmful information and adequately protects and backs up communication channels. While harmful information may spread online, responses might be most effective when they combine online and offline measures, especially through direct engagement with parties to a conflict, and particularly with the affected communities and people.

**RECOMMENDATION 21**

Humanitarian organizations should develop responses to harmful information against civilians in their operations.

Humanitarian organizations should strive to detect signals of the spread of harmful information against civilians in contexts where they operate. They should be aware of the risks and consequences such information may cause for conflict-affected populations, provide accessible and reliable information to facilitate access to humanitarian assistance and protection, and contribute to self-protection and resilience building of affected people in conflict settings. If appropriate, they should invest in building awareness and dialogue with actors that conduct information operations on the applicable international rules that protect civilian populations. At the same time, humanitarian response to harmful information must not amplify harmful information or cause unintended harm. In addition, humanitarian organizations should act with the necessary caution to ensure that their work to protect civilians from harmful information does not affect belligerents’ perception of their impartial, neutral, and independent humanitarian work.

**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.

A wide range of state and private actors (including private hackers and groups, as well as companies) have conducted cyber and other digital operations seemingly in support of parties to armed conflicts. Building on their experience in engaging with all parties to armed conflicts, humanitarian organizations should strengthen efforts to spread knowledge of the limits that IHL sets on digital operations. In addition to engaging with states on their obligation to ensure that private actors comply with IHL (see Recommendation 9), 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 such groups are sufficiently organized. In addition, humanitarian organizations – in collaboration with states and tech companies – should seek partnerships with engineering schools to make future operators aware of the specific rules applicable when conducting digital operations during armed conflict and the associated risks.
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.

Only a multidimensional and multistakeholder response can effectively protect civilians against digital threats during armed conflict, while safeguarding and promoting IHL and human rights law in the digital space. We recommend multistakeholder dialogue to develop conflict-specific and international law-based principles or guidelines for states and tech companies to combat digital threats, including harmful information. Dedicated research should be continued and supported to better document the scale of the problems, the harm that is caused, and refine the identification of solutions that comply with, and strengthen, IHL and human rights law.

We encourage the ICRC to provide a neutral space and facilitate confidential dialogue between states and other actors on the protection of civilians from digital threats during armed conflict to foster an exchange of views, strive to build alignment on various perspectives, and seek a common understanding of legal limits and practical protection measures.

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

Tech companies and humanitarian organizations should work together to develop concrete crisis protocols to ensure timely responses to digital threats against civilians, humanitarian organizations, and other protected actors. We also call on tech companies to assist humanitarian organizations by sharing their unique insights into digital threats on systems and platforms they develop and by providing support in areas such as cyber security, data protection, and innovation. Where necessary, companies that run digital platforms should promote impartial, accurate humanitarian information for populations in need. Such cooperation should consider humanitarian organizations’ working procedures, in particular the principles of impartiality, neutrality, and independence.

Tech companies and humanitarian organizations should inform and consult states as needed to protect civilian populations.

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.

Humanitarian organizations should partner with public and private institutions (academic, research, and expert institutions, as well as companies) to adapt existing products and services, or develop new ones, to protect civilians against digital threats and address the specific challenges to impartial humanitarian work in crisis contexts. 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.
THE WAY FORWARD

The use of digital technologies during armed conflict is only likely to grow. Civilians rely on such technologies as part of their daily lives; states digitalize their governance systems; tech companies continue to create new products and services; and humanitarian organizations need digital technologies to ensure effective and efficient operations for people in need. At the same time, belligerents will continue to use digital technologies for military purposes. It is our collective responsibility to ensure that digital technologies will be used responsibly and in compliance with international law. As states, the private sector, and civil society are discussing our common future in a digital age, the specific needs and risks faced by people affected by armed conflict and other humanitarian crises must be considered, prioritized, and effectively addressed.

We call on the international community 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. We hope our joint work and recommendations – which bring together policy, legal, and technological expertise – will be a call to action to this effect.
MEMBERS OF THE ICRC’S GLOBAL ADVISORY BOARD ON DIGITAL THREATS DURING ARMED CONFLICTS

**Dapo Akande**, professor of Public International Law, co-director of the Oxford Institute for Ethics, Law, and Armed Conflict, the Blavatnik School of Government, University of Oxford

**Tom Burt**, corporate vice-president, Customer Security and Trust, Microsoft


**Vice-Admiral (ret.) Arnaud Coustilliére**, cyber and digital senior adviser, Str@t-Algo, formerly commander of the French Ministry of the Armed Forces COMCYBER

**Camille François**, senior director for trust and safety at Niantic

**Marina Kaljurand**, member of the European Union Parliament for Estonia, former minister of foreign affairs for Estonia

**Irene Khan**, United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression

**Xiaodong Lee**, founder and CEO, Fuxi Institution, vice chairman of Internet Society of China, research professor of Chinese Academy of Sciences, adjunct professor of Tsinghua University

**Doris Leuthard**, former president and federal councillor of the Swiss Confederation, Switzerland

**Patricia Lewis**, research director, Conflict, Science and Transformation; director, International Security Programme, Chatham House

**Elina Noor**, senior fellow in the Asia Program at Carnegie Endowment for International Peace

**Gulshan Rai**, former national cyber security coordinator, government of India in the Office of Prime Minister of India

**Mariana Salazar Albornoz**, Universidad Iberoamericana, Ciudad de México, formerly member of the Interamerican Juridical Committee and special rapporteur for data protection and for international law applicable to cyberspace

**Dmitry Samartsev**, CEO, BI.ZONE

**Marijetje Schake**, international policy director at Stanford University Cyber Policy Center; international policy fellow at Stanford’s Institute for Human-Centered Artificial Intelligence

**Mirjana Spoljaric** (chairperson), president of the International Committee of the Red Cross

**Johanna Weaver**, director, Tech Policy Design Centre, Australian National University, formerly Australia’s independent expert and lead cyber negotiator at the United Nations

**Marcus Willett**, senior cyber adviser, International Institute for Strategic Studies, formerly director for cyber and deputy head of the United Kingdoms’ Government Communications Headquarters (GCHQ)
DEFINITIONS AND CONCEPTS

Armed conflict – The board focused specifically on digital threats during armed conflict. The board was guided by the understanding of the notion of “armed conflict” under international humanitarian law (IHL), i.e. armed conflicts between states (“international armed conflicts”) and armed conflicts between a state and a non-state armed group, or between such groups (“non-international armed conflict”). On several issues, however, the board makes recommendations that should be implemented in times of peace, for instance because they are similarly relevant outside armed conflict, because it is not always clear when a digital threat is linked to an armed conflict or a build-up thereof, or because the recommendation aims to build general resilience against digital threats.

Civilian – The board focused on the protection of civilian populations, civilian objects, and civilian data against digital threats. In line with IHL, it understands “civilians” as all people who do not belong to the military, and “civilian objects” as infrastructure, data, and other objects that do not qualify as military objectives. While focusing primarily on the protection of civilians, some recommendations also address the protection of other persons and objects during armed conflict, such as detained or wounded soldiers or military medical facilities.

Cyber operation – The board understood the term “cyber operation” as operations against a computer, a computer system or network, or another connected device, through digital means. The board considered primarily cyber operations that are conducted as a means or method of warfare in the context of an armed conflict.

Digital threats – The board focused on “digital threats”. This includes primarily threats arising from (often overlapping and mutually reinforcing) ‘cyber operations’, and ‘information operations’. In addition, it also encompasses risks of harm to civilians and civilian infrastructure arising from civilian involvement in armed conflicts using digital means. While referring to “digital threats”, the board was clear that such threats may also have consequences in the “offline world”.

Digital operations related to an armed conflict – The board used the term “digital operation related to an armed conflict” to address a range of digital operations related to digital threats that are conducted in the context of and with a link to an armed conflict.

Harmful information – The board understood “harmful information” as comprising information that has the potential to lead to physical or psychological harm to people during armed conflict in violation of IHL or human rights law, or that is otherwise likely to have harmful effects on civilians. It did not focus on the depiction of the information (i.e. as misinformation, propaganda, disinformation, or hate speech). In the assessment of harm, the board underlines the need to consider factors such as gender, age, literacy, or disability.

Information operation – The board understood the term “information operation” as the employment of information and communication technologies or other digital means to influence perception, motives, attitudes, or behaviour of adversaries or civilian populations to achieve political and military objectives. A cyber operation, as defined above, can contribute to an information operation. The board considered primarily information operations that use digital technologies and are conducted as a means or method of warfare in the context of an armed conflict.

Tech companies – The board used the term as an umbrella to refer to companies that provide digital platforms, services or infrastructure (including cyber security services), as well as internet service providers.
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.