Power of humanity

34th International Conference
of the Red Cross and Red Crescent

28–31 October 2024, Geneva

Protecting civilians and other protected persons and objects against cyber and information operations during armed conflict

BACKGROUND DOCUMENT

April 2024

EN

IC34/24/XX
Original: English
For information

Document prepared by the International Federation of Red Cross and Red Crescent Societies and the International Committee of the Red Cross

BACKGROUND DOCUMENT

Protecting civilians and other protected persons and objects against cyber and information operations during armed conflict

EXECUTIVE SUMMARY

The present resolution aims to address some of the dangers to civilian populations and other protected persons and objects arising from cyber and information operations in situations of armed conflict. It seeks to build a common understanding of the opportunities provided by the availability and reliability of information and communication technologies (ICTs) during armed conflict, and the dangers that the use of ICTs for cyber and information operations poses, and to identify concrete measures to address some of these dangers. The resolution calls on States and the components of the International Red Cross and Red Crescent Movement (Movement) to take steps to these ends.

The availability and reliability of ICTs provides opportunities in the social, economic, development, and information and communication realms. In times of armed conflict, ICTs can save and improve lives. For instance, ICTs enable people to survive by finding out where they can get food, water and blankets and a safe place to stay, and allows them to contact and find family members they have lost contact with. At the same time, the use of ICTs for military purposes during armed conflict can bring new dangers for the lives, safety and dignity of civilians and other protected persons and objects. Of especial concern are cyber and information operations directed against civilian populations and other protected persons and objects, with particular dangers arising from operations that target medical facilities and humanitarian operations.

To address some of these dangers, the resolution recalls the consensus among States that international humanitarian law (IHL) only applies to situations of armed conflict, recognizing the need for further study into how and when IHL applies to the use of ICTs, such as cyber and information operations. Subsequently, the resolution recalls some of the cardinal IHL rules and principles on the protection of civilian populations, demands their effective implementation, and calls on States to uphold their obligations to respect and protect medical personnel, units and transports (i.e. vehicles) in all circumstances and to allow and facilitate, as well as to respect and protect, humanitarian relief activities. In this context, the resolution suggests inviting States and Movement components to welcome the research led by the International Committee of the Red Cross (ICRC) – in consultation with external experts and the other Movement components – on a possible "digital emblem", and encourages further work on this subject.

The resolution also recalls the responsibility of Movement components to take appropriate steps, within the scope of their respective mandates, capacities and operational needs, to bolster their ability to maintain appropriate levels of cyber security and data protection.

1) INTRODUCTION

The availability and reliability of information and communication technologies (ICTs) provides opportunities in the social, economic, development, and information and communication realms, and can save and improve lives. During armed conflict, ICTs enable people to survive by finding out where they can get, for instance, food, water and blankets and a safe place to stay, and allows them to contact and find family members they have lost contact with. ICTs also have the potential to enable humanitarian organizations to deliver humanitarian relief more efficiently, and may allow belligerents, for example, to provide effective warnings and improve reconnaissance for the protection of civilians. At the same time, the use of ICTs for military purposes during armed conflict can bring new dangers for the lives, safety and dignity of civilians and other protected persons and objects.

The ICRC, together with Movement partners, has been at the forefront of conducting research and holding expert consultations on the potential human cost of cyber and information operations during armed conflict. Recognizing these risks, and consistent with our mandate, the ICRC is working for the understanding and dissemination of knowledge of IHL, including with regard to new means and methods of warfare. States have worked in United Nations forums on ICTs in the context of international security and the protection of human rights. Since 2019, there has been an increased focus in the Movement on risks related to the protection of data in humanitarian operations, in particular against data breaches.

The proposed resolution, put forward in the unique humanitarian forum afforded by the International Conference of the Red Cross and Red Crescent (International Conference), aims to draw attention to the need to protect civilian populations and other protected persons and objects against cyber and information operations, and identify measures that States and members of the Movement may take to prevent or minimize such harm.

2) BACKGROUND

The proposed resolution will be the first time the International Conference addresses the use of ICT capabilities during armed conflict, in particular cyber and information operations. It will build on resolutions of the International Conference and the Council of Delegates that focused on data protection, as well as reports produced by the ICRC jointly with experts from all parts of the world, on the protection of civilians against digital threats.

Regarding the protection of humanitarian data, the proposed resolution aims to build on the resolution "Restoring Family Links while respecting privacy, including as it relates to personal data protection", adopted at the 33rd International Conference in 2019, as well as the measures agreed by components of the Movement in the resolution "Safeguarding humanitarian data", adopted at the 2022 Council of Delegates. The "Handbook on Data Protection in Humanitarian Action" may also be of further interest.

Regarding the potential human cost of cyber and information operations, and practical measures States and humanitarian organizations should consider, the ICRC would like to draw delegations' attention in particular to the 2023 report of the ICRC's Global Advisory Board on Digital Treats During Armed Conflicts. The board brought together a global group of policy, legal, military and technological leaders. Its report presents four guiding principles and 25 concrete recommendations for belligerents, States, tech companies and humanitarian organizations to prevent or mitigate digital threats to civilian populations.[1] As the proposed resolution also addresses ICRC-led research on a possible "digital emblem", the report Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Solutions may be of particular interest.

3) ANALYSIS/PROGRESS

In places affected by armed conflict and other emergencies, people often rely on the availability and reliability of ICTs to access goods and services that are essential to their survival and well-being. ICTs allow governments to provide essential services to populations and maintain

[1] Additional ICRC publications that may be of interest include ICRC, The Potential Human Cost of Cyber Operations, 2019; ICRC, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021; ICRC, Harmful Information: Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence, 2021.

civilian governance. The confidentiality, integrity and availability of ICTs, and of the data they rely on, is also essential for the functioning of medical services – both military and civilian – and an increasingly critical element of humanitarian operations, including those of the Movement. At the same time, ICTs are also used nowadays as a means or method of warfare, in particular in the form of cyber and information operations. This reality creates significant questions and challenges for the protection of populations affected by conflict and for principled humanitarian action.

A) Dangers to civilian populations arising from cyber and information operations

Building on its observations in contemporary armed conflicts and the research and consultations mentioned above, four types of dangers are particularly relevant, owing to their likelihood and potential negative impact on civilians.

Cyber operations
The more our daily lives rely on ICTs, 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. Cyber operations designed to manipulate information for cognitive 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.

Information operations
Information operations have long been part of armed conflict. They are 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 information ecosystems and platforms, distorting facts, influencing people's beliefs and behaviours, raising tensions and increasing the risk 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 may negatively affect the availability, integrity and reliability of critical information that civilians need for their safety and survival in times of conflict. Compared to legacy media, digital platforms often do not have sufficient editorial oversight or content moderation capabilities, enabling harmful information to spread more easily. Civilians may also unknowingly spread harmful content, further amplifying its potential scope and impact.

Civilians getting drawn into cyber and information operations
Civilians – as individuals, in groups or in corporations – have long been relied upon to perform military functions during armed conflict and to assist in the war effort. With the digitalization of societies, the types of operations they can conduct and the number of civilian actors that get involved in armed conflict are increasing. This development comes with frequently overlooked risks for civilian populations: the more digital technologies draw civilians towards hostilities, the greater the risk of harm they are exposed to. The more digital infrastructure or services are shared between civilians and armed forces, the greater the risk of civilian infrastructure being attacked.

Cyber and information operations directed against medical facilities and humanitarian organizations

For several years, the ICRC has grown increasingly concerned that, as digitalization increases, medical facilities are becoming vulnerable to cyber operations and to incidental harm from such operations directed elsewhere. Likewise, new dangers are arising from disinformation spread by digital means and aimed at undermining the life-saving work of medical services, putting medical personnel at risk. The potential human cost of cyber and information operations is particularly acute during armed conflicts and other emergencies, when medical services are urgently needed.

At a time marked by huge numbers of people in need and insufficient humanitarian response capacity, cyber and information operations against humanitarian organizations risk having devastating consequences for the populations who need their protection and assistance to survive. In recent years, Movement components have become victims of such operations. These operations can take different forms, from cyber operations that disrupt or destroy humanitarian organizations' digital infrastructure to operations that penetrate their systems to exfiltrate data, to disinformation operations that undermine their reputation and endanger their ability to operate.

For medical and humanitarian actors alike, data breaches risk not only putting lives and livelihoods at risk, but also undermining the trust that civilians and parties to armed conflicts place in them, which affects their access to people and can put the safety of their personnel at risk.

B) A collective response from the Movement and States party to the Geneva Conventions

To respond to the dangers identified above, the proposed resolution pursues two main objectives.

First, in the preambular paragraphs, it aims to build a common understanding of some of the risks of harm to civilian population and other protected persons and objects that are posed by cyber and information operations during armed conflict. The resolution puts particular emphasis on the risk of cyber operations disrupting ICTs that are part of or are used by critical civilian infrastructure and essential services; information operations inciting violence and hatred in violation of IHL; the specific dangers that cyber and information operations pose to medical services and humanitarian operations, including their data; and the challenges and risks that arise when civilians are encouraged to conduct – or tolerated if they conduct – cyber or information operations during armed conflict.

Second, in the operational paragraphs the resolution recalls the consensus among States that IHL only applies to situations of armed conflict, recognizing the need for further study how and when IHL applies to the use of ICTs, such as cyber and information operations. Subsequently, the resolution recalls cardinal IHL principles on the protection of civilian populations, demands their effective implementation and calls on States to uphold their obligations to respect and protect medical personnel, units and transports (i.e. vehicles) in all circumstances, and to allow and facilitate, as well as to respect and protect, humanitarian relief activities and personnel. In addition, the resolution encourages all Movement components to integrate the protection of civilian populations and other protected persons and objects during armed conflict into their operational, policy and legal work, and to take appropriate steps, within the scope of their respective mandates, capacities and operational needs, to enhance their ability to ensure appropriate levels of cyber security and data protection in all areas of their work. On these issues, the resolution calls for collaboration with and support by States.

One avenue to enhance the protection of medical and humanitarian activities against the dangers arising from cyber and information operations may be the ICRC-led research on a possible “digital emblem”; that is, a digital means of identifying the digital infrastructure and data of organizations and entities that are entitled to display the distinctive emblems recognized under international humanitarian law. On this subject, the resolution aims to welcome the work done thus far by the Movement and in consultation with States and other experts, and encourages further work on this subject.

4) RESOURCE IMPLICATIONS

By adopting this resolution, States and Movement components commit to take appropriate steps, within the scope of their respective mandates, capacities and operations, to enhance the protection of civilian populations and other protected persons and objects during armed conflict. The resolution also expects Movement components to take appropriate steps to enhance their ability to ensure appropriate levels of cyber security and data protection. Furthermore, the resolution encourages the ICRC to further research and test the technical feasibility of a digital emblem and to consult with States and Movement components.

The implementation of these commitments may have resource implications for States or Movement components, depending on the extent of their existing legislation, policies, programmes and activities.

5) IMPLEMENTATION AND MONITORING

The success of this resolution depends on States and Movement components implementing agreed measures in their own legislation, policies, programmes and activities. States are expected to do so as part of their implementation of IHL and policies on the protection of civilian populations. Movement components are expected to implement relevant parts of the resolution as part of their efforts on data security and personal data protection, as is feasible and appropriate, as well as IHL dissemination.

All members of the International Conference are invited to report to the next International Conference on the progress made in implementing this resolution.

6) CONCLUSION AND RECOMMENDATIONS

In the year of the 75th anniversary of the adoption of the four Geneva Conventions, the present resolution aims to address the changing realities of armed conflict. It seeks to build a common understanding and identify concrete measures to address some of the threats posed by cyber and information operations to civilian populations and other protected persons and objects during armed conflict. It calls on States and Movement components to take steps to this effect, within their respective responsibilities.

Adopting this resolution will be a landmark in the ongoing international efforts to ensure that the use of ICTs enhances the well-being of people. It will focus specifically on the protection needs of people affected by armed conflict. Being adopted in the unique forum afforded by the International Conference, and having a distinct humanitarian focus on protecting civilians and medical and humanitarian actors in situations of armed conflict, the resolution will stand apart, and complement, intergovernmental efforts in multilateral forums.