

DRAFT FOR FIFTH STATE CONSULTATION

Workstream 6 – UPHOLDING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING ARMED CONFLICTS

CO-CHAIRERD by Ghana, Luxembourg, Mexico, Switzerland and the International Committee of the Red Cross

Overview

Information and communication technologies (ICTs) have become essential to the lives of people throughout the world. In our digitalized and connected world, essential services for civilian populations, as well as people’s ability to connect with loved ones and pursue economic development, depend on the integrity and availability of ICTs. In conflict-affected areas, reliable ICTs are critical for civilians to access essential goods and services, for governments to provide services, and for supporting medical services and humanitarian activities, including those of the International Red Cross and Red Crescent Movement. While ICT capabilities may enable belligerents to achieve military objectives without necessarily causing harm, or with less harm to civilians or civilian objects than kinetic operations, their use in contemporary conflicts has also given rise to harmful ICT activities affecting civilian populations, data and infrastructure, including across international borders. Disparities in technological capacities and cybersecurity resilience may further exacerbate such risks, including by affecting the ability of states and other relevant stakeholders to prevent, mitigate and respond to harm arising from ICT activities during armed conflict.

The workstream underscored the imperative to protect civilian populations and preserve human dignity in contemporary and future conflicts. To this end, it is essential to uphold and strengthen respect for international humanitarian law (IHL) in the use of ICTs during armed conflicts to protect civilian infrastructure, networks, communications and data against harmful ICT activities during armed conflict.

In their use of ICTs, states must comply with international law, in particular the Charter of the United Nations, including the obligation to settle international disputes by peaceful means and the prohibition of the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations. Nothing in IHL can be construed as legitimizing or authorizing any act of aggression or any other use of force inconsistent with the Charter of the United Nations. The application of IHL does not legitimize or encourage conflict.

The workstream also identified good practice and produced practical recommendations, outlined below, notably to

- protect the civilian population and civilian data and infrastructure from harmful ICT activities
- safeguard medical services and humanitarian activities from digital threats, and uphold prohibitions on sexual violence and the recruitment and use of children in hostilities, including through online means
- address the spread of information in violation of IHL
- minimize the risk of harm to the civilian population arising from the military use of civilian ICT infrastructure and prevent civilians – from hackers to personnel of technology companies – involved in ICT activities from violating IHL or from inadvertently putting themselves at risk.

The workstream further underlined the importance of the following overarching elements in strengthening the protection afforded by IHL in relation to ICT activities:

- recognizing that, in conflict-affected areas, reliable ICTs are critical for civilians, governments and humanitarian actors, and that ICT activities can inflict human costs even without causing physical damage, underscoring the need to uphold humanity and human dignity in war
- committing to promote and clarify the application of IHL to ICT activities, and to take all necessary measures, individually and collectively, to mitigate risks to the civilian population and ensure that ICT activities remain consistent with the protections afforded by IHL
- continuing the study and discussion of how IHL applies to ICT activities, building on discussions under the workstream and this outcome document, with a view to further building and promoting a shared understanding that safeguards civilians from harm
- promoting transparency through the public sharing of national views on how international law, including IHL, applies to ICT activities, as well as the exchange of lessons learned and good practices on mitigating civilian harm
- supporting capacity-building at bilateral, regional and global levels to strengthen states' ability to implement and apply IHL in relation to ICT activities.

Outcome

1. Protecting the civilian population and civilian data and infrastructure from harm arising from ICT activities during armed conflict

Contemporary armed conflicts show that ICT activities can pose risks to the civilian population and civilian data and infrastructure. Such activities can seriously affect civilians and other protected persons and objects, including where essential services – namely services vital to ensuring the subsistence of civilian populations, as well as all those interrelated systems on which people depend to meet their basic needs – such as electricity, water, sanitation, food production and distribution, telecommunications, health care, education, humanitarian and emergency services or financial services, are disrupted, even in the absence of physical damage.

In the conduct of ICT activities in the context of and associated with an armed conflict, compliance is required at all times with IHL, including but not limited to the principles of humanity, military necessity, distinction, proportionality and precautions.

ICT operations reasonably expected to cause death or injury to persons, or to result in damage to or destruction of objects, amount to attacks under IHL. This includes operations that are reasonably expected to disable ICT systems and require action to restore their functionality. Such ICT operations must be conducted in accordance with all IHL principles and rules on the conduct of hostilities, including the prohibitions on attacks against civilians and civilian objects, indiscriminate attacks and disproportionate attacks, and the principle of precautions.

Data lies at the heart of an increasingly digitalized world and plays a central role in the functioning of essential civilian services and humanitarian activities. The way data is handled during armed conflicts may affect people's lives and dignity. Medical, biometric, financial and humanitarian data, among others, are integral to the delivery of public and social services. Deleting, manipulating, denying access to, or disclosing such data without authorization may disrupt essential services and expose individuals and communities to serious harm. Information-gathering activities *per se* are not prohibited under IHL, including when they involve accessing data.

Several IHL principles and rules offer protection to the civilian population and civilian data and infrastructure against the dangers arising from ICT activities during armed conflicts, including:

- the principles that the right of the parties to armed conflict to choose methods or means of warfare is not unlimited, and that a party to an armed conflict may only resort to those means and methods of warfare that are necessary to weaken the military forces of the enemy
- the principles and rules governing the conduct of hostilities, including the principles of distinction, proportionality and precaution and the related prohibitions on attacks against civilians and civilian objects, indiscriminate attacks and disproportionate attacks
- the obligation to take constant care to spare the civilian population, individual civilians and civilian objects in the conduct of military operations
- the rules protecting property from pillage, seizure and destruction.

The following measures, which reflect a combination of existing law and good practices, are particularly important to strengthen the protection of the civilian population and civilian data and infrastructure from harm arising from ICT activities during armed conflict:

- a) Establish and apply rigorous procedures for ICT operations to ensure compliance with IHL, including to verify that targets qualify as military objectives and are not subject to special protection, and to assess and avoid or at least minimize the risk of incidental civilian harm.
- b) Base ICT operations including targeting procedures on all reasonably available information actively sought from relevant sources, including reliable data and intelligence, which are supported by legal advice, as required under IHL; and to the maximum extent feasible, seek expertise from cybersecurity and other relevant technical specialists on the structure, interconnectivity and civilian dependencies of ICT infrastructure.
- c) Where ICT infrastructure qualifies as a military objective under IHL but continues to serve civilian functions, take into account all reasonably foreseeable direct and indirect incidental harm on the civilian population, data and infrastructure resulting from the total or partial loss of its civilian use and the consequent impact on civilian services it provides or enables, in accordance with the principles and rules of proportionality and precautions in the planning and conduct of attacks.
- d) In implementing the obligation of taking all feasible precautions in the choice of means and methods of warfare, select those means and methods that are expected to cause the least incidental civilian harm, including by rigorously assessing whether ICT-enabled or other non-kinetic means and methods would reduce the risk of civilian harm compared to available kinetic alternatives.
- e) Apply appropriate geographic, temporal and system-based limitations (“fencing”) in the conduct of ICT operations, to avoid, or at least minimize, the risk of incidental civilian harm.
- f) Continuously monitor ICT operations and ensure the ability to adjust or terminate them to prevent unintended or excessive civilian harm. Where feasible, incorporate technical safeguards, such as kill switches, to enable the halting, limiting or isolation of ICT operations if they risk spreading beyond their intended target, including to civilian networks or infrastructure or those of third-party states.
- g) Take all appropriate measures to conduct ICT activities that are supported or enabled by artificial intelligence or other emerging technologies in a manner consistent with IHL and with the measures above.

2. Minimizing the risk of harm to the civilian population arising from military use of civilian ICT infrastructure during armed conflict

Except for certain military networks, the ICT environment is predominantly civilian. However, the interconnection between civilian and military networks, and military use of civilian ICT infrastructure, create specific challenges for their protection.

Where civilian ICT infrastructure including infrastructure provided by technology companies is used for military purposes, not every such use renders it, or even parts thereof, a military objective under IHL. Nevertheless, military use may increase the risk that such infrastructure will be attacked, thereby exposing civilians and civilian objects in physical proximity to, digitally connected to, or dependent upon it to incidental harm.

IHL prohibits attacking civilian objects, including civilian ICT infrastructure. However, military use may turn such infrastructure, or parts thereof, into military objectives only for such time as they meet the

criteria stipulated under IHL. Such determinations require particular care and a case-by-case assessment.

When attacking such military objectives, states and parties to armed conflict must respect the prohibitions on indiscriminate and disproportionate attacks and the principle of precautions, including where the civilian population relies on that ICT infrastructure for the delivery of essential services. All feasible precautions must be taken to conduct attacks in a manner that affects only those components or functions of the ICT infrastructure used for military purposes, and to avoid, and in any event minimize, damage to those serving civilian functions.

To protect the civilian population against the effects of attacks, states and parties to armed conflict must, to the maximum extent feasible, take all necessary precautions to protect civilians and civilian objects under their control from the dangers arising from military operations.

In addition to the measures set out in Outcome 1 above, the following measures, which reflect a combination of existing law and good practices, are particularly important to minimize the risk of harm to the civilian population arising from the military use of civilian ICT infrastructure during armed conflict:

- a) Allocate appropriate financial and technical resources and adopt planning, design and configuration measures in advance of and during armed conflict, with a view to minimizing the exposure of civilians and civilian ICT infrastructure to the effects of ICT activities during armed conflict.
- b) To the maximum extent feasible, physically or technically separate the components of ICT infrastructure used for military purposes from those serving civilian functions, including through network segmentation or other appropriate configuration measures. This includes, to the maximum extent feasible, segregating data used for military purposes from those serving civilian needs, such as through separate storage and management and access-control arrangements.
- c) Strengthen the resilience of essential civilian ICT infrastructure and services, including through redundancy, contingency-planning and other measures to reduce the risk of incidental civilian harm.

3. Minimizing risks related to the involvement in ICT activities during armed conflict of civilians on the territory of a state or under its jurisdiction or control

In today's armed conflicts, the involvement of civilians in ICT activities during armed conflicts has become more pronounced. In some situations, states have tolerated, facilitated or encouraged civilians to conduct ICT activities against the adversary, including activities that may affect civilians and civilian objects.

As civilians are drawn closer to hostilities, they risk exposure to harm. Many may be unaware of the risks involved, the potential legal consequences of their conduct, or the IHL rules they need to follow.

Civilians – from hackers to personnel of technology companies – must comply with IHL and other applicable law when conducting ICT activities in the context of and associated with an armed conflict.

Under international law, states and parties to armed conflicts are responsible for IHL violations committed by civilians whose ICT activities during armed conflict are attributable to them, including hackers and personnel of technology companies. States must take all appropriate measures to prevent

IHL violations from being committed through or facilitated by the ICT activities by civilians on their territory or under their jurisdiction or control, and to suppress such violations if they do occur. States undertake to disseminate IHL as widely as possible in order to make IHL known to civilians in their respective countries. They must not encourage, aid or assist civilians in violating IHL, including through ICT activities.

Civilians are protected against attack unless and for such time as they take a direct part in hostilities. Under certain limited circumstances, civilian involvement in ICT activities may amount to direct participation in hostilities. In order to avoid the erroneous or arbitrary targeting of civilians, parties to armed conflict must take all feasible precautions in determining whether a person is a civilian and, if so, whether they are directly participating in hostilities, including through ICT activities. In case of doubt, IHL requires that the person be presumed to be protected against attack.

Children must not be allowed to take part in hostilities during armed conflict, including through ICT activities.

The following measures, which reflect a combination of existing law and good practices, are particularly important to minimize risks related to civilian involvement in ICT activities during armed conflict:

- a) Take appropriate steps to inform civilians who may be involved in ICT activities in the context of and associated with an armed conflict of the legal and practical risks of doing so. These could include sharing information about IHL rules via social media, dedicated applications, radio or other means of mass communication, or developing IHL-compliant model codes of conduct that civilians conducting ICT activities should be asked to follow.
- b) Avoid, to the extent feasible, involving civilians in ICT operations amounting to direct participation in hostilities, to protect them from the dangers resulting from military operations. Where such participation nevertheless occurs, integrate civilians into the armed forces to the extent feasible.
- c) Take all feasible measures to prevent children from taking part in hostilities through ICT activities, for example through education and awareness programmes for children and caregivers; by adapting the national legislation and policies prohibiting the recruitment and use of children to address online means, and enforcing them; and by considering age restrictions on access to digital tools that could amount to direct participation in hostilities, where appropriate.

4. Protecting civilian ICT products and services provided by technology companies during armed conflict

ICT products and services provided by technology companies are widely used by the civilian population, governments and impartial humanitarian organizations, including during armed conflicts. Their disruption, degradation or misuse can therefore have significant humanitarian consequences. Such ICT products and services, as well as the civilian personnel providing them, are protected under IHL.

At the same time, technology companies increasingly provide cybersecurity and other ICT services or products to parties to armed conflict, which may result in the loss of their protection afforded under IHL. In such situations, civilians and civilian objects that rely on such products and services may also be exposed to harm.

In order to enhance the protection of civilian ICT products and services provided by technology companies during armed conflict, technology companies should:

- a) Duly consider that providing ICT products and services to parties to armed conflict carries both legal and practical risks.
- b) Understand, assess and take measures to minimize the risks of harm to civilians and civilian objects, whether to the personnel or property of these companies, or due to their physical proximity, digital connection to, or dependence upon the relevant infrastructure or services. This includes, to the extent feasible, physically or technically separating their infrastructure, services and products used to support military operations from those used for civilian purposes.
- c) Take measures to prevent their personnel from engaging in, facilitating or otherwise becoming involved in conduct amounting to violations of IHL, including through the provision of ICT products or services to parties to armed conflict, and to take appropriate action should any such situations occur.

5. Safeguarding medical services, humanitarian activities and other specifically protected persons, objects and activities from harm arising from ICT activities during armed conflict

The health-care sector and impartial humanitarian organizations are especially vulnerable to ICT activities during armed conflict. The increasing reliance of medical and humanitarian services on interconnected systems and digital data means that disruptions to ICT infrastructure or services can directly affect life-saving medical operations, compromise sensitive data, impair the work of impartial humanitarian organizations and their personnel, and jeopardize the delivery of assistance.

Medical personnel, units and transports, as well as humanitarian personnel and objects, must be respected and protected at all times, in accordance with IHL, including from harm arising from ICT activities. ICT activities during armed conflict must not unduly disrupt the functioning of medical services and humanitarian activities, including their data, ICT and communication systems.

The confidentiality of medical and humanitarian data must be respected, in accordance with IHL. This protection is critical to preserve trust in the work of medical services and impartial humanitarian organizations.

Parties to armed conflict must also take all feasible measures, in the prevailing circumstances and in light of the resources available to them, to prevent medical services and humanitarian activities from being harmed, including through ICT activities by third parties such as cyber criminals and other non-state actors not attributable to a party to an armed conflict, in accordance with IHL and other applicable international law.

Certain other objects and activities benefiting from specific protection under IHL, including objects indispensable to the survival of the civilian population, works and installations containing dangerous forces, cultural property and civil defence, may also face grave risks from ICT activities. The specific protection accorded to them must be respected, including when conducting ICT activities during armed conflicts. This protection includes their data and the ICT infrastructure indispensable to their functioning.

ICT activities can be used to commit or facilitate acts of sexual violence or to recruit or use children in hostilities. IHL prohibits sexual violence and the recruitment and use of children in hostilities, including when such acts are committed through or encouraged or facilitated by ICT activities.

The following measures, which reflect a combination of existing law and good practices, are particularly important to safeguard medical services, humanitarian activities and other specifically protected persons, objects and activities from harm arising from ICT activities during armed conflict:

- a) Support discussions and efforts to make the specific protection afforded under IHL to medical services and humanitarian activities identifiable and visible in the ICT environment, including through the development of a “digital emblem”, and continue engaging with the ICRC on the legal, technical and diplomatic avenues for its implementation.
- b) Explicitly reaffirm their commitment to respecting and protecting medical services and humanitarian activities, including the data, ICT and communication systems of these services and activities, and to facilitating their operations in the ICT environment, as well as to respecting the specific protection for objects indispensable to the survival of the civilian population, including their data and the ICT infrastructure indispensable for their functioning. Such commitments should be reflected in national law, policy, military doctrine and practice.
- c) Where feasible, support and facilitate the development of adequate cybersecurity and data protection measures for medical service providers and impartial humanitarian organizations, and assist in strengthening their resilience to ICT threats affecting their systems and operations.
- d) Strengthen relevant national legal and policy frameworks addressing online conduct that may constitute or facilitate violations of IHL, including, among others, those related to sexual violence and to the recruitment or use of children in armed conflict, and ensure effective implementation and coordination among relevant authorities. Particularly to prevent unlawful recruitment and use of children, broader governmental efforts should be undertaken to educate children and caregivers about the associated risks.
- e) Integrate specific safeguards into military doctrine, standard operating procedures and rules of engagement to prevent and address violations committed through or facilitated by ICT activities, including sexual violence and the recruitment or use of children in hostilities. Measures, where feasible, include regulating the use of personal ICT devices in operational settings, restricting the sharing of sensitive images or information, and prohibiting the use of ICTs to unlawfully recruit or involve children in hostilities.

6. Addressing the spread of information in violation of IHL

In contemporary armed conflicts, ICT activities are increasingly used to spread information that may violate IHL. While information operations have long formed part of warfare and are not unlawful *per se*, the use of ICTs, particularly through social media platforms or messaging applications or when combined with artificial intelligence and other emerging technologies, can significantly amplify the speed, scale and reach of harmful information.

States and parties to armed conflict must refrain from, and take all feasible measures to prevent, the spread of information in violation of IHL, including through the use of ICTs. This includes spreading information that incites or encourages IHL violations, exposes persons deprived of liberty to insults or

public curiosity, or whose primary purpose is to spread terror among the civilian population. In certain specific circumstances, the spread of information constitutes or facilitates perfidy.

Medical services and humanitarian activities must be protected from ICT-enabled disinformation which obstructs their work during armed conflict. Such acts unduly interfere, and are incompatible with, the obligation to respect and protect medical and humanitarian personnel and their activities.

The following measures, which reflect a combination of existing law and good practices, are particularly important to address the spread of information in violation of IHL:

- a) Take all feasible measures to assess, prevent and mitigate the risk of information operations, including when supported or enabled by artificial intelligence or other emerging technologies, harming the civilian population and other protected persons, including by undermining their safety, dignity or access to essential services.
- b) Refrain from spreading information that dehumanizes the adversary or propagates hatred against the civilian population, including through ICTs, and take appropriate measures to ensure that their armed forces, other public authorities, or persons acting on their behalf do not engage in such conduct.
- c) Support, where feasible, medical service providers and impartial humanitarian organizations in building capacities to strengthen resilience against disinformation and other harmful information activities, including by facilitating their ability to gather, verify and disseminate accurate information in line with their medical or humanitarian activities; strengthening their preparedness and contingency-planning to address exposure to harmful information; and encouraging the development of context-appropriate responses to harmful information affecting civilians within their areas of operation.
- d) Engage with relevant actors, including the technology sector, to reduce the risk that online platforms or other ICT services are used to incite, encourage or facilitate violations of IHL or otherwise harm civilians and civilian objects. This may include developing appropriate legal and policy frameworks and promoting the adoption by technology companies of safeguards and practices designed to detect, assess and address harmful information in situations of armed conflict.
- e) Endeavour to strengthen societal resilience to harmful information activities, including by supporting the availability of reliable information, protecting journalists and media where required by IHL and other applicable law, and promoting preparedness measures that enhance the ability of the civilian population to access trustworthy information during armed conflict.
- f) Refrain from shutting down civilian access to the internet or other ICT services unless justified by imperative military necessity, as such measures risk harming the civilian population. Where such restrictions are imposed, take mitigation measures to minimize adverse effects on civilians to the greatest extent possible.

7. Cross-cutting measures to strengthen the implementation of IHL in relation to ICT activities

The following cross-cutting measures, which reflect a combination of existing law and good practices, are particularly important to strengthen the implementation of IHL in relation to ICT activities, including in peacetime:

- a) Disseminate IHL knowledge within armed forces and among the wider population, particularly among those who may be involved in ICT activities, and integrate IHL principles and rules and their application to ICT activities into national legislation, military doctrine, standard operating procedures, rules of engagement, codes of conduct and training, as appropriate.
- b) Make available qualified legal advisers to military units and commands responsible for ICT activities, particularly in the planning and conduct of such operations.
- c) Conduct legal reviews of ICT capabilities that function as new weapons, means or methods of warfare in their study, development, acquisition or adoption, to ensure that their employment, would not, in some or all circumstances, be prohibited by international law. Such reviews should be conducted through, *inter alia*, rigorous testing, evaluation, verification and validation of ICT capabilities, to better understand their functioning, propagation and potential effects on civilian systems.
- d) Adopt all necessary legislative, regulatory and other measures, including, where appropriate, penal sanctions, to prevent and suppress IHL violations committed through or facilitated by ICT activities by persons or on territory under their jurisdiction or control.
- e) Take appropriate measures during the design, development and deployment of ICT capabilities to reduce the risk of their unintended spread, repurposing, reengineering or misuse in ways that may amount to or contribute to violations of IHL, including through appropriate cybersecurity safeguards, such as encryption, and technical measures, such as built-in kill switches, to limit their propagation or unauthorized reuse.
- f) Promote voluntary information-sharing and confidence-building measures aimed at reducing risks to civilian ICT infrastructure, including exchanges of good practices among states, the establishment of communication channels and other practical risk-reduction arrangements, and, where appropriate, voluntary reporting of significant ICT incidents that have caused unintended civilian harm, in order to enhance collective understanding and risk mitigation.
- g) Promote transparency and shared understanding through the development and public sharing of national views on how international law, including IHL, applies to ICT activities, including in the form of national or common positions, and through the exchange of lessons learned and good practices to minimize civilian harm.
- h) Support capacity-building at bilateral, regional and global levels to strengthen states' ability to implement and apply IHL in relation to ICT activities.
- i) Foster cooperation among states, technology companies, impartial humanitarian organizations and civil society to use ICTs in ways that enhance the protection of civilians, including through the development of context-specific guidance or practical arrangements.
- j) Encourage cooperation between technology companies and impartial humanitarian organizations to improve preparedness and response to ICT threats affecting protected persons and objects, including through information-sharing and cybersecurity support, while respecting the humanitarian principles of neutrality, impartiality and independence.
- k) Integrate gender- and age-sensitive, and disability-inclusive approaches into national frameworks and operational practice in order to strengthen the implementation of IHL, including in identifying and addressing ICT-related risks.