HUMANITARIAN
LAW & POLICY

Offline and in danger: the humanitarian consequences of connectivity disruptions

July 1, 2025, Access / Analysis / Communications / New Technologies / Social Protection

11 mins read

Cléa Thouin
Advisor on Protection in the Digital Age, the ICRC Delegation for Cyberspace & Global Cyber Hub

As people around the world become increasingly reliant on digital and telecommunications networks to access essential services, contact loved ones, and seek help, the rising number of connectivity disruptions in armed conflicts is a growing source of concern for their safety and dignity.

In this post, ICRC Protection Specialist Cléa Thouin reflects on the humanitarian consequences of such disruptions – situations in which digital or telecommunications become partially or completely lost – and on the need to address their causes and mitigate their impact, especially in contexts where connectivity can mean the difference between life and death.

ICRC Humanitarian Law & Policy Blog · Offline and in danger: the humanitarian consequences of connectivity disruptions

How much of your life depends on connectivity? As societies become increasingly digitalized, connectivity, and particularly access to the internet, now plays an increasingly important role in many people's daily lives – from the mundane aspects like the platforms providing us with entertainment to more essential tasks such as staying in touch with loved ones, communicating at work, making medical appointments and carrying out financial transactions. So, when connectivity is disrupted during times of conflict or crisis, the stakes can be very high. In these moments, connectivity is no longer just a matter of convenience. It can save lives.

Without connectivity, when military operations start, it may be near impossible to get accurate and life-saving information on safe evacuation routes, or about areas affected by hostilities. Individuals trying to cross international borders to seek protection may not be able to request or access essential documents stored online. People in areas affected by disruptions may be left without financial resources to purchase essential goods when mobile cash stops functioning, and families may be left without news about the fate of loved ones.

In recent years, the devastating impact of connectivity disruptions on conflict-affected people and communities has been highlighted by many organizations, including *Access Now*, the UN Office of the High Commissioner for Human Rights (*OHCHR*), the Global System for Mobile Communications Association (*GSMA*), and the *ICRC*. In light of their increasing incidence, it is key for the humanitarian sector to better understand and address the causes and consequences of connectivity disruptions in order to provide an effective humanitarian response to affected populations.

In conflict settings, connectivity disruptions can happen for a number of reasons. Often, this can be as an incidental effect of hostilities, such as when maintenance crews are unable to safely reach conflict-affected areas to repair or maintain physical infrastructure enabling connectivity, or when the consumables needed to power connectivity, in particular electricity or fuel, experience shortages or as a result of supply chain disruptions.

Deliberate connectivity restrictions, where disruptions are the result of intentional or targeted measures,[1] are *increasingly* observed in conflict settings, with actors targeting both connectivity in areas under their own control and in areas under the control of others. For example, authorities and other actors can implement technical disruptions, notably by ordering or pressuring Internet Service Providers (ISP) to interrupt internet connectivity. Cyber-attacks on ISPs or telecommunication companies and physical acts of sabotage can also lead to disruptions in connectivity. Military operations can intentionally damage or destroy physical infrastructure needed for connectivity, such as cell phone towers or fiber optic cables. Electromagnetic measures such as jamming can also be deployed to affect connectivity for the duration of military operations or more permanently.

An additional threat to people's lives, safety and dignity

In *Ethiopia*, *Gaza*, *Myanmar*, *Sudan* and other places, connectivity disruptions have had profoundly disruptive impacts on people affected by armed conflict. As is often the case, children, women, elderly persons, persons with disabilities, or displaced people and migrants are disproportionately affected.

When connectivity is disrupted, communities have fewer avenues to seek and receive potentially life-saving *information* about ongoing hostilities, safe evacuation routes, and the availability and location of shelter, essential services, and medical or humanitarian aid. This lack of visibility increases their risk of being exposed to violence and physical harm or of suffering from untreated injuries and illnesses. The *risk* of mis- and disinformation spreading can also increase when reported facts cannot easily be checked against reliable sources, exposing people to further dangers or turning them away from protection and assistance.

With no internet, communities also have fewer means to *organize* their own responses and to communicate their needs to authorities and humanitarian actors, reducing their resilience to crisis and potentially leaving them without much-needed assistance for prolonged periods of time. In many settings, and particularly in rural or hard-to-reach areas, communities often depend on connectivity to *contact emergency services* such as ambulances or rescue services, increasing the risk of preventable deaths and exposing people to danger when they take it upon themselves to seek help elsewhere. Lack of connectivity can also impair people's ability to retrieve or seek to obtain important documents and certificates before evacuating conflict-affected areas, making it harder for them to cross frontlines or international borders to seek safety or international protection.

The delivery of essential services can be disrupted or made unreliable, as critical infrastructure that enables essential public services now often use and depend on connectivity to operate. Water, wastewater, and electricity *infrastructure* may not function normally or even be rendered inoperable, with significant risks for public health. Already overstretched hospitals and health services providers may not be able to access patient files, organize surgeries or provide *on-call expertise* without reliable connectivity. In remote areas where *telemedicine* can bring critical help, communities may be left without access to health altogether. National or local warning and notification systems, including for natural disasters, can also be impacted by lack of connectivity, leaving populations unprepared to deal with emergencies.

Connectivity disruptions prevent families separated across frontlines or international borders from staying in touch, often at times when hostilities are at their most intense, leaving them unable to confirm the fate of their relatives and increasing the risk of persons going missing. This can have a significant psychological toll, adding to the stress, anxiety and traumas of living through conflict.

In places where digital learning tools have emerged as *key solutions*, access to education is often jeopardized when connectivity is disrupted, preventing students from registering for university, attending classes or taking exams. Connectivity restrictions have also widely been reported to impact people's livelihoods and their access to economic opportunities. In many conflict-affected countries, a large number of people increasingly depend on digital financial services such as *mobile cash* and remittances from abroad, both of which have been severely impacted by connectivity restrictions. In addition, many households in violence-affected areas rely on online businesses for their livelihoods, meaning that internet disruptions can *leave* them without income sources. In such circumstances, connectivity 'black markets' can emerge around alternative sources of connectivity, often *benefitting* armed or criminal groups, fueling conflict dynamics and creating additional protection risks for conflict-affected people seeking alternative sources of connectivity.

While the humanitarian consequences of connectivity disruptions can be significant, it's important to acknowledge that connectivity itself can also expose people to risks. Authorities, belligerents and others sometimes use it to surveil, persecute and target people, and marginalized communities can also face further obstacles and be exposed to discrimination through connectivity. Furthermore, under human rights law, states may restrict access to communication networks when legitimate and proportionate security reasons justify it. These considerations create '*digital dilemmas*' for humanitarian actors who need to *navigate* the opportunities and risks that connectivity can bring for people affected by conflict, to ensure that they '*do no digital harm*' in their advocacy and assistance. But the growing dependence of people and societies on connectivity means that the cost of disruptions has never been so high.

Disrupting a critical enabler for humanitarian action

Humanitarian organizations, too, increasingly depend on connectivity to deliver responses at the speed and scale required by emergencies. Connectivity disruptions can hamper their ability to operate and provide *assistance*.

Humanitarians often rely on connectivity to identify humanitarian needs, for example when they remotely collect information from hospitals on casualty numbers during emergencies or when they contact affected populations for individual follow up. They use it to carry out remote documentation of potential violations of international law (including through OSINT and *remote technologies*) and to conduct real-time, life-saving interventions. They also need connectivity to *coordinate* internally and to run logistical and supply chains. Security can also be impacted: at a time when humanitarian workers have *never* faced as many threats to their lives, connectivity disruptions can threaten their ability to obtain crucial security guarantees for field teams or simply to reach relevant stakeholders in times of need. When alternatives such as *satellite connection* exist, they can be comparatively costly, their use is not always permitted under national law, and sometimes they carry political and surveillance risks, meaning that they are not always easily scalable.

During connectivity disruptions, humanitarians can also come under increased monitoring to ensure that they do not bypass restrictions. In parallel, they can face additional pressure to provide information about what they see on the ground to fill the information vacuum on possible violations of international humanitarian and human rights law. Their ability to preserve their independence and the confidentiality of the sensitive information they need to protect people is at stake. And yet, maintaining a principled approach is not an option but a functional requirement.

Building a better way forward

At the 34th International Red Cross and Red Crescent Movement Conference, states and components of the Movement adopted by consensus a *resolution* to better protect civilians against the potential human cost of Information and Communication Technology activities during armed conflict. It explicitly recognizes the importance of connectivity for the protection of civilians and principled humanitarian action and calls for "the protection of critical infrastructure essential to the general availability or integrity of the internet." This is an important achievement considering the sometimes polarized debate on these issues. More importantly, it creates a concrete basis for states and other stakeholders to discuss and find solutions to mitigate the humanitarian impact of connectivity disruptions in the future.

There are different avenues that can help structure and guide legal, policy, protection and operational efforts to ensure that connectivity disruptions do not cost or harm lives. Humanitarian diplomacy and advocacy, as well as protection dialogue with belligerents, should highlight the consequences of connectivity disruptions and include calls for stronger respect notably for international humanitarian law and human rights law. Efforts should also focus on how to design connectivity infrastructure in a way that facilitates the distinction between civilian and military digital assets and data and on how to reinforce the robustness and resilience of connected systems, both from a technical and a *socio-political* point of view. Looking at their own operations, humanitarian organizations should think about how to deliver effective humanitarian solutions in low and no connectivity settings and reflect on the *risks, advantages and nuances* of providing connectivity as aid. In parallel, authorities should consider how to preserve humanitarians' ability to use connectivity for emergency and lifesaving operations by granting them adequate protection or connectivity privileges and immunities.

We have never had as many technological and sophisticated means at our disposal to ensure our ability to communicate when the lives, safety and dignity of populations are at stake. States, non-state armed groups, the private sector and other actors that have the power to trigger connectivity disruptions must consider the humanitarian impact of their decisions, and take action to prevent civilian death, injury, and suffering.

References

[1] These kinds of disruptions are often referred to as ‘internet shutdowns’, a term defined and popularized by the digital rights organization Access Now as “intentional disruptions of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.”

See also:

- Joelle Rizk, *Why is the ICRC concerned by ‘harmful information’ in war?*, September 10, 2024.
- Chris Brew, *From content to harm: how harmful information contributes to civilian harm*, February 27, 2024.
- Megan O’Brien, *Online violence: real life impacts on women and girls in humanitarian settings*, January 4, 2024.
- Susanna Acland and Barnaby Willitts-King, *Mobile phones for participation: building responsible public-private humanitarian partnerships*, December 7, 2023.
- Rakesh Bharania and Mark Silverman, *Protective by design: safely delivering connectivity as aid*, July 8, 2021.

Tags: armed conflict, Civilians, communications, Cyber and Information Operations, modern warfare, protection, Techplomacy

You may also be interested in:

Photographing humanity: hope amid crisis in Myanmar

7 mins read

Access / Analysis / Communications / New Technologies / Social Protection Stephanie Xu

When a powerful earthquake struck Myanmar on 28 March 2025, it tore through communities already …

Respect for the dead under Islamic law: considerations for humanitarian forensics

21 mins read

Access / Analysis / Communications / New Technologies / Social Protection Ahmed Al-Dawoody

In contemporary humanitarian crises, handling the dead presents significant practical and ethical challenges. With a …