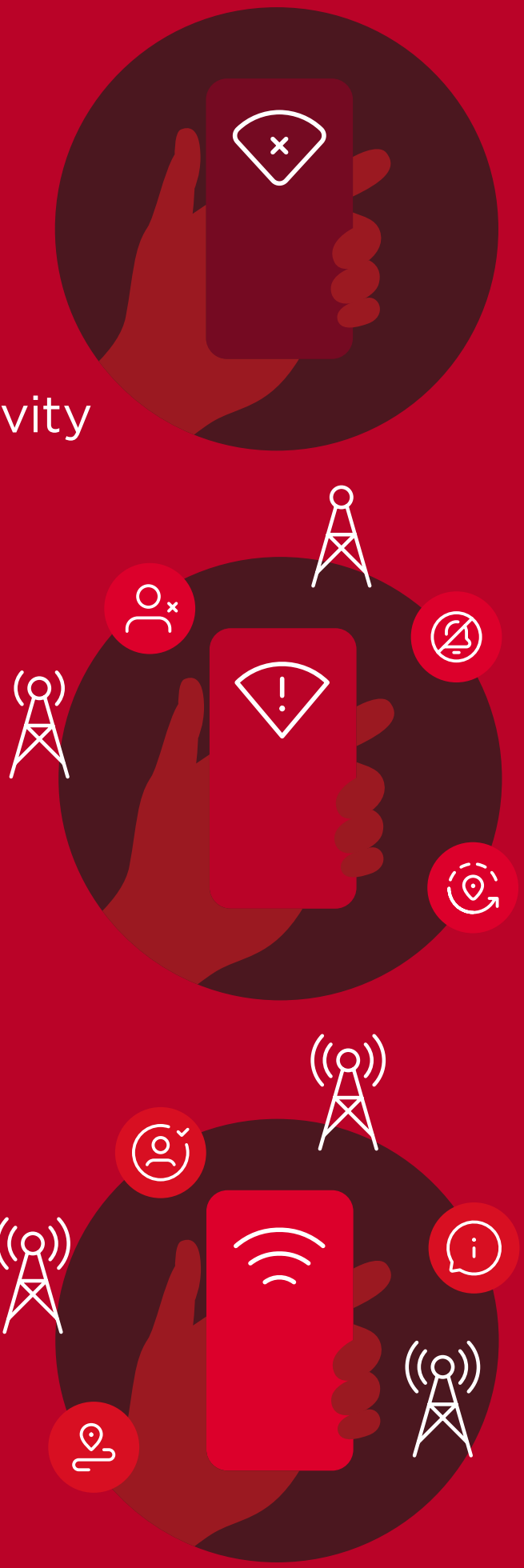
GSMA

January 2024

Connectivity in Crisis: The Humanitarian Implications of Connectivity for Crisis-Affected Communities



GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at www.gsma.com

Follow the GSMA on Twitter/X: @GSMA

GSMA Mobile for Humanitarian Innovation

The GSMA Mobile for Humanitarian Innovation programme works to accelerate the delivery and impact of digital humanitarian assistance. This is achieved by building a learning and research agenda to inform the future of digital humanitarian response, catalysing partnerships and innovation for new digital humanitarian services, advocating for enabling policy environments, monitoring and evaluating performance, disseminating insights and profiling achievements.

Learn more at www.gsma.com/m4h or contact us at m4h@gsma.com

Follow GSMA Mobile for Development on Twitter/X: @GSMAm4d

Authors

Matthew Downer, Senior Insights Manager, Mobile for Humanitarian Innovation

Zoe Hamilton, Senior Insights Manager, Mobile for Humanitarian Innovation

Acknowledgements

GSMA contributors from Public Policy, Security, Digital Inclusion, Mobile for Humanitarian Innovation, Mobile for Development

Colleagues from several partner organisations who gave their time to be interviewed.

Special thanks go to colleagues from Access Now, Cyberpeace Institute, International Committee of the Red Cross (ICRC) and Internews for providing immensely valuable peer review on drafts of this report.

This initiative has been funded by UK International Development from the UK government and is supported by the GSMA and its members.

The views expressed do not necessarily reflect the UK government's official policies.

Contents

Introduction	2
1. No connectivity: the humanitarian coverage gap	6
2. Lost or limited connectivity	13
3. Stable connectivity: connected crises	19
4. Human and structural factors affecting connectivity	25
Conclusion	29
References	30

Introduction

Connectivity, both the presence and absence of it, has profound implications in crisis settings. Increasingly part of prominent humanitarian policy discussions, there is a growing understanding that connectivity, and the access to information it provides, is a fundamental requirement for both crisis-affected communities and an effective, modern humanitarian response.

Connectivity has drastically changed the way in which crisis affected people live their lives and the ways that humanitarians provide assistance. It enables people to connect with loved ones, look for solutions and fulfil their aspirations. It also allows them to access information and services on their own terms, including where provided by humanitarians, strengthening resilience to shocks in the short term and supporting greater autonomy and self-reliance in the long term. However, while the connectivity needs of humanitarian responders tend to be met in a crisis, the corresponding needs of crisis-affected communities are often underappreciated, under-supported and poorly understood.

This report focuses on the humanitarian implications of connectivity and the risks it poses, including the lack or loss of connectivity during a crisis. Our analysis aims to foster a deeper understanding of the risks and opportunity costs of connectivity and how to better address them, pragmatically and with crisis-affected communities at the centre.

In an increasingly connected world, it is vital to understand and articulate these risks and opportunity costs. Connectivity is not a risk-free panacea, and the humanitarian community needs to be realistic about how connectivity intersects with conflict, natural hazards and forced displacement, creating and exacerbating risks and vulnerability for crisis-affected communities around the world. However, while humanitarian actors are right to be mindful of the potential harms of connectivity, being unconnected brings its own risks.

As more and more of our lives are lived online, it is also pertinent to explore the ways in which humanitarian principles apply in the digital space. For example, how can digital personhood be protected as the effects of conflicts and disasters are also experienced online? As humanitarian actors explore how their operations extend to the digital world, the obligations of humanitarian actors should also be examined.

While this report does not provide definitive answers to these questions, it does spark a conversation about the role of the humanitarian sector in these new digital realities. What is the responsibility of the sector to extend connectivity? How is connectivity changing the nature of humanitarian crises more broadly, and what is the role of the sector in responding to that change and addressing the new risks that have emerged?

We hope this analysis will help to bring the sector together to discuss these pressing questions and begin to build consensus on the best way forward.

About this report

Building on extensive research related to the opportunities and potential benefits of connectivity[1] in humanitarian crises, both by the GSMA[2] and other key players such as the UN Refugee Agency (UNHCR),[3] this report focuses on the potential implications, risks and opportunity costs of the lack, loss, or presence of connectivity for crisis-affected communities. Those who are new to these topics should read this analysis alongside existing research on the potential opportunities and benefits of connectivity, as this will provide a balanced view of how stakeholders can be enabled to do more, rather than encouraged to do less, in the digital space.

In this report, "humanitarian crises" are defined as shocks that cause widespread human suffering, including conflict, acute food insecurity, forced displacement and natural hazards.

1 In this report, "connectivity" is defined as the presence or use of 2G, 3G, 4G or 5G networks.
2 For example, Casswell, J. (2019). The Digital Lives of Refugees. GSMA; GSMA and UNHCR. (2022). The Digital Worlds of Displacement-Affected Communities.
3 For example, UNHCR. (2016). Connecting Refugees.

While the collation of these implications in one place represents a novel analysis, it is not the first time these questions have been asked. An increasing number of blogs, articles and studies have looked at the growing dependence on connectivity in crisis situations, the effects of damage to network infrastructure[4] and the humanitarian impacts of service restriction orders (SROs),[5] among other issues. There is consensus that the humanitarian implications of connectivity are far reaching, and that more evidence is needed. We hope this report creates a fuller picture and a deeper understanding of the impact and implications of connectivity in humanitarian settings.

In this report, we have intentionally not proposed solutions or ways to mitigate connectivity risks, nor have we highlighted existing technological approaches or the limitations of connectivity. This will all be explored in future GSMA work.

The position of the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation that helps business and society thrive. Representing the interests of more than 1,000 mobile network operators (MNOs) and other organisations across the sector, the GSMA is a proponent of connectivity as a force for good in the world. We believe connectivity can enable people, industry and society to thrive, and we support tackling today's biggest challenges.

The GSMA is also an active voice in support of humanitarian connectivity. For more than 10 years, there has been a programme of work focusing on the role of connectivity in crises, from natural hazards to forced displacement and conflict. The GSMA is also a member of global humanitarian initiatives, such as the Emergency Telecommunications Cluster (ETC), the CALP Network and the Risk-informed Early Action Partnership (REAP), and works actively with dozens of humanitarian organisations, from UN agencies to international and local non-governmental organisations (NGOs).

While this paper is based on a robust and objective research methodology and has been reviewed by external partners, it is important to acknowledge the position of the GSMA in discussions on connectivity in crisis and how it may influence the positions we take.

Methodology

This report is envisaged as the beginning of a programme of work and engagement. As an initial landscaping and framework development exercise, we conducted a desk-based analysis that included an extensive literature review and a round of key informant interviews (KIIs) with participants who were identified through existing connections and snowball sampling.

For the initial desk review, the M4H team compiled resources that covered content from one of four categories: closing mobile coverage gaps; the impacts of SROs; the impacts of misinformation, disinformation and hate speech (MDH) online; and the humanitarian implications of connectivity services. This was then refined into three overarching categories (see the next section). More than 100 documents were included in the review and stored, tagged and summarised in a custom Airtable sheet.

A summary of the desk review was used to identify key gaps in the available evidence, again structured around the three categories of connectivity. These gaps were used to develop an interview guide, which the team used to conduct interviews with 22 colleagues from UN agencies, NGOs, academia and the private sector. We acknowledge that not engaging directly with members of crisis-affected communities is a methodological flaw. However, subsequent reports in this series intend to validate these findings with people affected by crisis and to bring their opinions and experiences into these discussions in a meaningful way.

4 For example, ICRC. (2023). Protecting Civilians Against Digital Threats During Armed Conflict.

5 For example, Jaspers, S., Murdoch, C. and Majid, N. (2022). Digital feast and famine: Digital technologies and humanitarian law in food security, starvation and famine risk.

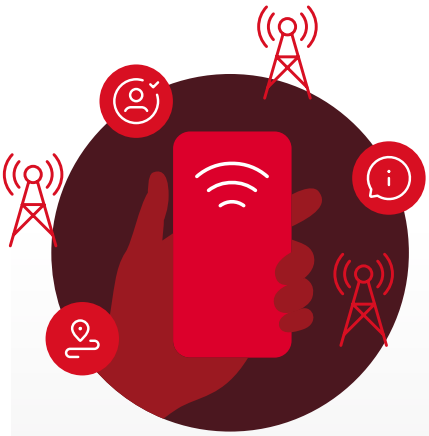
About this analysis

This analysis articulates and categorises the humanitarian implications of connectivity, including the risks and, to some extent, the opportunity costs. Three states of connectivity are considered relevant to humanitarian crises and analysed in this report: not being covered by a mobile network; losing connectivity or having limited connectivity; and having an available network. All three states are examined in greater detail in this report.

However, such neat categorisation oversimplifies the reality of connectivity in crisis. For example, the availability of mobile networks is not an either/or state – even when a network is physically available, it may be intermittent, unreliable or lack the necessary bandwidth to cope with demand. Similarly, communities living outside a mobile network may travel to areas with coverage as part of their daily routine, with information easily communicated between community members. Access to, and use of, connectivity also depends on many factors, including functioning energy systems, handset ownership and user demand and digital skills. These considerations and others are explored in detail in chapter 4.

Unconnected / uncovered

Lost or limited connectivity



Covered / connected

The humanitarian implications of connectivity

Within these states of connectivity, we identified numerous humanitarian implications, both risks and opportunity costs, and grouped them into five categories: Protection, Information ecosystem, Humanitarian aid and coordination, Autonomy and Well-being.

These groupings are neither neat nor perfect, with several implications falling under more than one theme.

Similar implications also appear in multiple states of connectivity, with variation and nuance to how they are experienced by people affected by crisis. However, these categories are useful in looking at broader considerations and helping to understand and identify the best ways to mitigate potential connectivity-related risks. Each of these categories is defined and briefly summarised below.

Protection

A scenario in which there is potential for harm to individuals affected by crisis.

Harm may be intrinsic in the risk itself, such as violence or human rights violations. Harm may also be a related consequence of the risk, such as the inability to receive a warning message and take appropriate action, leaving someone in harm's way.

Digital protection

The term "digital protection" is increasingly popular in the humanitarian sector, reflecting a shift in the understanding of protection concerns to include those that originate or manifest in digital spaces. However, the use of this term is multifaceted across the sector and is often linked directly to the specific mandates of protection agencies. The lack of a universally agreed definition makes it less useful as an analytical framework and, as such, has not been used in this report.

Humanitarian aid and coordination

The ability of humanitarian responders to deliver humanitarian assistance safely, effectively and efficiently to crisis-affected communities.

Information ecosystem

The quality, validity, confirmability and availability of information to crisis-affected communities.

Risks are primarily related to navigating the information ecosystem, the reliability of information or the ability to receive important messages. This category often covers issues related to misinformation, disinformation and hate speech (MDH).[6] Importantly, many risks in this category are closely aligned with protection, a relationship already noted by many humanitarian actors.[7]

Autonomy

The ability of individuals and communities to make decisions for themselves, to meet their own needs or to access products and services independently.

This includes, among other issues, access to personal finance, the strength of the local economy and breaking cycles of dependency on humanitarian assistance.

Well-being

Where risks are related to people's well-being, beyond basic survival.

This includes mental health or the ability to pursue leisure activities or other needs often excluded from humanitarian analyses.[8]

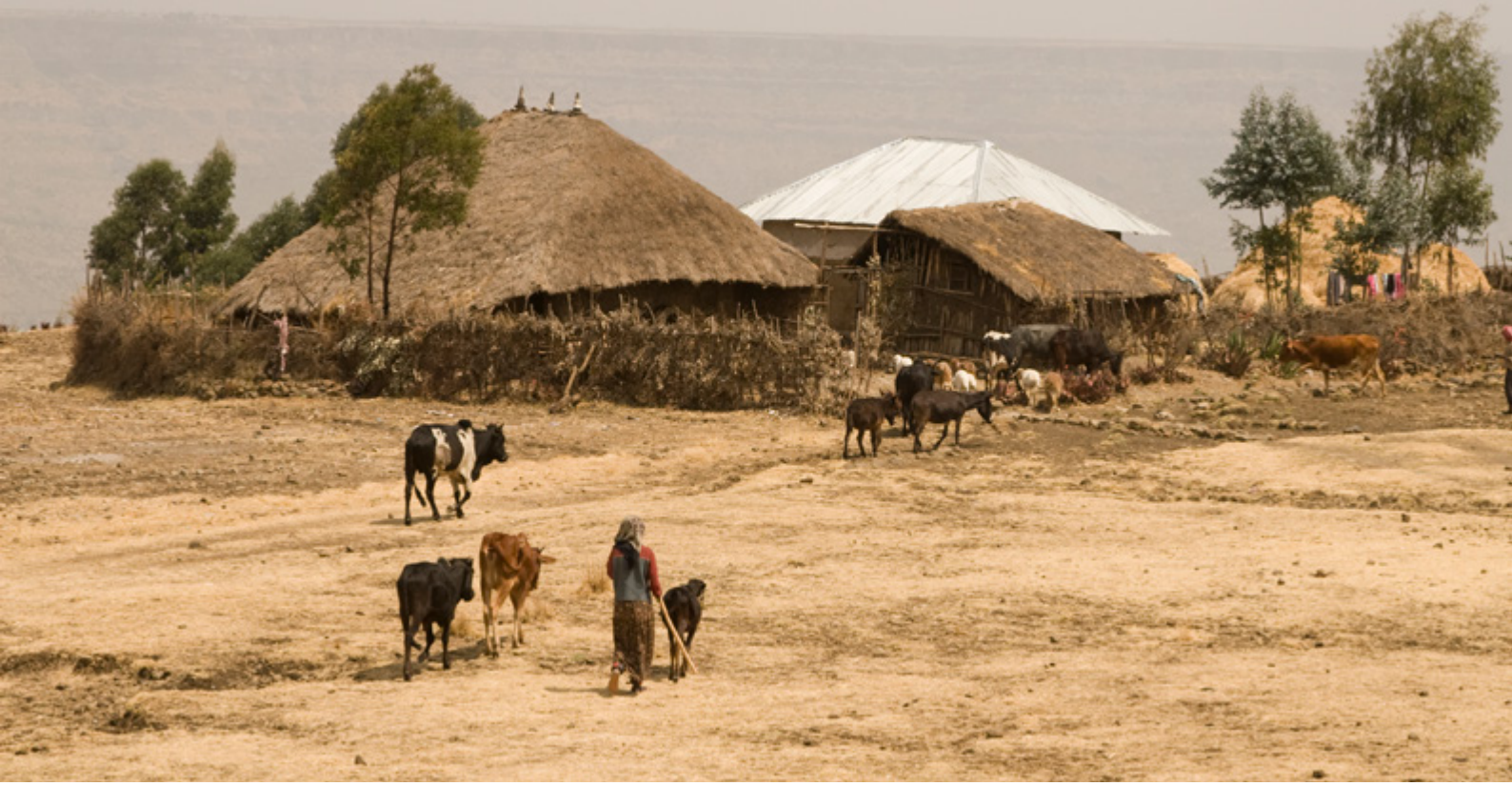
6 "Misinformation" is false information that is spread unintentionally. "Disinformation" is false information that is intentionally fabricated and shared with bad intent. "Hate speech" is all forms of print, audio and visual content that is spread to incite or promote hate, aggression and/or violence against specific groups or identity traits. (Source: ICRC, 2021).

7 Internews. (2023). Information and Risks: A Protection Approach to Information Ecosystems.

8 Lough, O. et al. (2023). Beyond survival: exploring wellbeing in humanitarian action. Overseas Development Institute (ODI).

01

No connectivity: the humanitarian coverage gap



In modern crises, what does it mean to have no mobile connectivity?

Despite the widely recognised potential benefits of mobile network coverage, data suggests that people affected by crisis disproportionately live in areas that do not have it. **In 2022, 15 of the 36 countries with the largest[9] mobile coverage gap[10] were experiencing protracted humanitarian crisis[11] and 29 had a heightened risk to extreme natural hazards.**[12] An estimated 172 million people are in need of humanitarian assistance in these 36 countries[13] and, despite accounting for only 13% of the global population, these countries host 46% of internally displaced people (IDPs)[14] and 18% of refugees.[15] This suggests that countries with the largest coverage gaps are more likely to be experiencing crisis, and that forcibly displaced people (FDPs) are more likely to live in areas without coverage.

Understanding the boundaries of connectivity infrastructure is essential to understanding and closing mobile coverage gaps. A 2016 UNHCR study found that, globally, refugees living in rural areas were twice as likely to not have mobile coverage than the global population.[16] However, this type of analysis is not widely available and there is no standardised approach.[17]

It is important to recognise that mobile "black spots", especially the notion of "bringing the internet to the unconnected", are an oversimplification. It is rare that a community would be completely without mobile services and unaware of the existence, benefits and uses of connectivity and internet services. Even in very remote and sparsely populated rural locations, which constitute most of the world's remaining uncovered areas, human mobility and word-of-mouth mean that at least some people are likely to have heard of the internet and may even own mobile phones to use technologies like Bluetooth or radio that do not require a network connection to work.[18] However, rural communities are overall less likely to be aware of mobile internet. For example, in 2022, only 46% of Ethiopia's rural population (which make up 77% of the country) were aware of the internet, compared to 79% of the urban population.[19]

9 Those with a coverage gap of more than 10%, or twice the global average of 5%. (Source: GSMA. (2023). The State of Mobile Internet Connectivity Report 2023.)
10 The proportion of people who live in an area not covered by a mobile network.
11 "Protracted crises" refer to countries that have had UN-coordinated country response plans or country components of regional response plans for at least five consecutive years in 2022.
12 Having high vulnerability to climate change, with low readiness. (Source: Notre Dame Global Adaptation Initiative. (2023). ND-GAIN Matrix.)
13 Development Initiatives. (2023). Global Humanitarian Assistance Report 2023.
14 Internal Displacement Monitoring Centre. (2022). Global Internal Displacement Database.
15 UNHCR. (2023). Refugee Data Finder.
16 UNHCR. (2016). Connecting Refugees.
17 ITU. (2020). The Last-mile Internet Connectivity Solutions Guide: Sustainable Connectivity Options for Unconnected Sites.
18 Key informant interview (KII), Technologist
19 GSMA. (2023). The State of Mobile Internet Connectivity Report 2023.

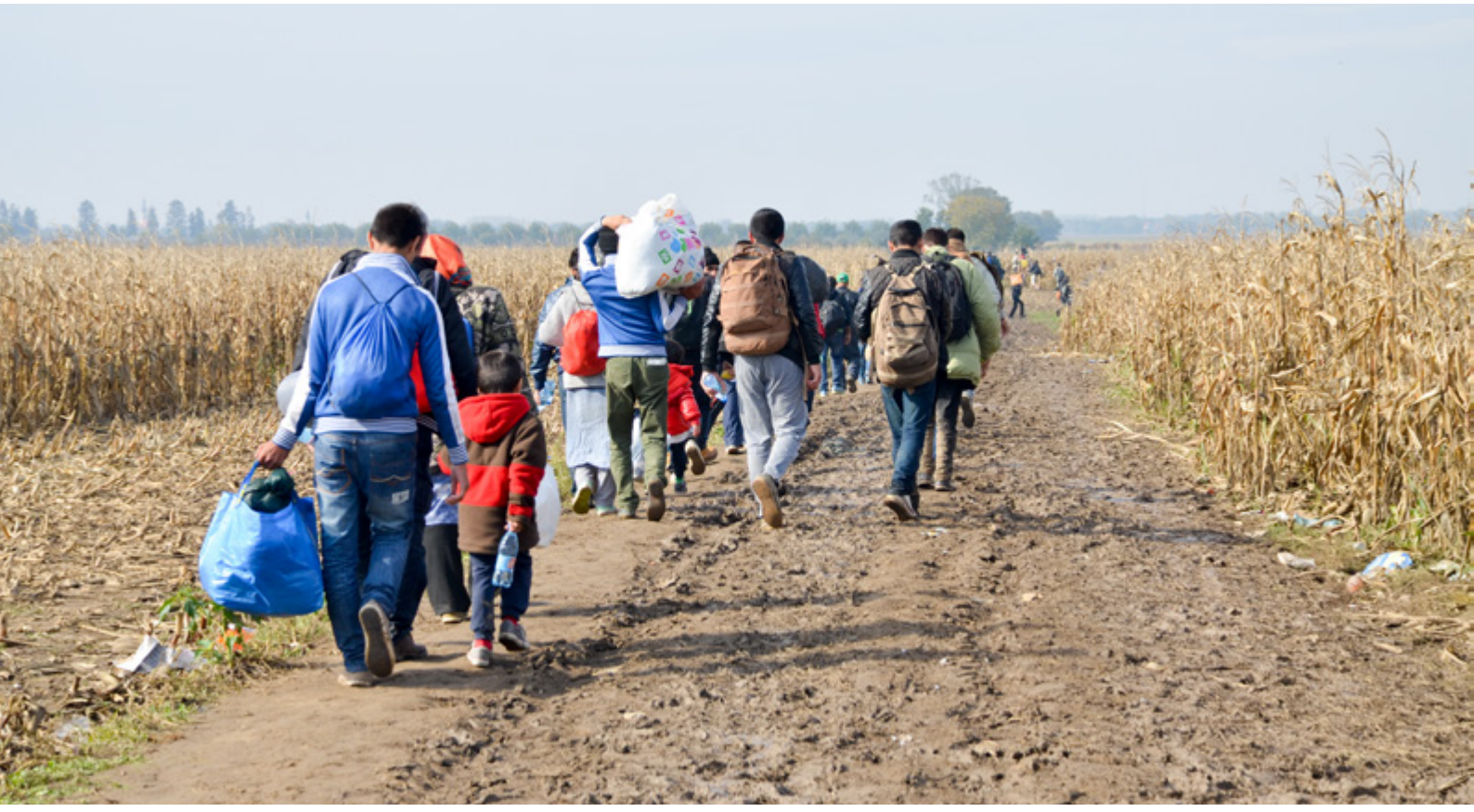
Access to connectivity, therefore, is not a simple matter of "haves" and "have nots". It is important to be aware of the dynamics influencing a person's access to, and awareness of, connectivity services, and how this affects their ability to communicate or access information or humanitarian services.

Still, this analysis considers uncovered communities as "unconnected" in order to illustrate the extremes and fully articulate the humanitarian imperative of closing mobile coverage gaps.

Expanding mobile networks to cover communities in need of assistance is not enough to remedy the risks and challenges faced by crisis affected people. **Reaping the full benefits of connectivity in a safe and dignified manner will take more than infrastructure.** It will also require holistic programming that addresses a range of dynamic factors.[20]

As the humanitarian sector continues to digitalise and services increasingly move online, allowing humanitarian coverage gaps to continue to exist will pose increasingly severe risks. It may even come into contention with the humanitarian principles of impartiality and do no harm, as people who are connected will be easier to reach and may increasingly receive a greater share of humanitarian assistance, further entrenching exclusion. **As such, this analysis of how coverage gaps intersect with crises not only helps frame the risks for individuals, communities and humanitarian responders, but also demonstrates that humanitarian actors may have a role in making the case for network expansion in crisis settings.**[21]

Historically, most aid agencies have worked within the realities of existing networks, accepting when no coverage is available and rarely advocating for expansion. In most cases, barring direct intervention, network expansion is driven by demand and other market forces. **Closing humanitarian coverage gaps will likely require new stakeholders, perhaps humanitarian or development actors, to stimulate or consolidate demand and make a compelling business case to network providers.** This is not a role that these sectors have traditionally played but, increasingly, coalitions and collaboration between humanitarian and development actors, the private sector and national policymakers and regulators have led to positive change.[22]



20 KII, Humanitarian

21 While this analysis focuses on understanding the risks and implications of humanitarian coverage gaps, a forthcoming paper focusing solely on this issue will examine potential models to close them.

22 KII, Humanitarian

Humanitarian implications

This analysis identifies humanitarian implications and risks of crises that occur in areas without mobile network coverage. While impactful and life-saving humanitarian assistance certainly existed before the advent and proliferation of connectivity, today risks can stem from poor programme design (for example, relying on digital tools in an offline environment) and the inability to get online and reap the benefits of connectivity.

Given the humanitarian implications of connectivity, there will increasingly be a humanitarian imperative to close the remaining mobile coverage gaps around the world. This will likely require cross-sectoral coalitions to advocate, support and drive change, and to galvanise action. An upcoming GSMA report will explore models through which the humanitarian sector might play a role.

Protection risks

1.1 Inability to raise concerns or ask for help

A lack of connectivity can increase feelings of personal insecurity, particularly the inability to quickly raise an alarm or ask for help in the face of danger.[23] Communities themselves are almost always the first responders, and connectivity can enable rapid assessments of damage and need, as well as coordination within the community. When a crisis occurs in an area without reliable network coverage, this assessment and coordination becomes more difficult. It can also create additional hurdles to communicating needs to authorities or humanitarian responders, which runs the risk of communities being left without additional support from national or international entities for extended periods.[24]

Mobile networks have also become powerful tools in reporting protection concerns, abuses or issues related to humanitarian assistance, or lack thereof. Many organisations are investing heavily in digital solutions that support accountability to crisis-affected communities.[25] Without connectivity, it becomes more difficult or impossible to report protection issues or human rights concerns.

In areas without connectivity, where agencies now have complaint and feedback mechanisms that rely on mobile technology, interviewees shared concerns that issues are not being reported and that some agencies are misinterpreting low engagement as evidence there are fewer issues to be addressed.[26]

23 Downer, M. (2019). Bridging the Mobile Gender Gap for Refugees. GSMA; UNHCR. (2016). Connecting Refugees.
24 KII, Humanitarian
25 Ibid.
26 Ibid.

1.2 Barriers to effective delivery of core humanitarian assistance

Humanitarian assistance is increasingly digital, with programming ranging from food distribution to water and sanitation (WASH) to family reunification services relying on connectivity.[27] In interviews with a range of humanitarian practitioners in countries such as the Democratic Republic of the Congo (DRC), Somalia and Sudan, they were quick to reflect on the multiple ways in which mobile coverage gaps had restrained or slowed the delivery of services to people who needed them.[28]

Mobile coverage gaps can also lead to people being excluded from humanitarian services.[29] When meaningful and timely engagement is made difficult through a lack of networks, the result can be poor programme design and the provision of poorly targeted assistance.[30] Even when services are well designed, the inability to share information effectively through digital channels can leave people unaware of the assistance to which they are entitled.[31] This can result in short-term harm, such as exclusion from food distributions or cash assistance, as well as more permanent harm, such as missing resettlement interviews.[32]

Taking this argument further, connectivity gaps that leave people without services may undermine the humanitarian principle of impartiality.[33]

1.3 Barriers to efficient humanitarian coordination

Mobile coverage gaps can mean a slower and less efficient humanitarian response, with poor coordination and duplication of efforts.[34]

Connectivity provides unparalleled opportunities for humanitarian responders to share information rapidly and coordinate during a crisis. Because connectivity has increasingly been used in this way, it is no longer acceptable for responses to be delayed by lags in communication while waiting for staff to reach sites where they can use a computer, radio or satellite phone to pass on information.[35] Outside areas of mobile connectivity, humanitarian responders are increasingly reliant on other forms of temporary connection, such as Very Small Aperture Terminals (VSATs), which can take time to arrive and, in many instances, are only available for use during the immediate crisis response.

In recent years, the humanitarian sector has demonstrated the efficiency gains that are possible with digital humanitarian assistance. A key example is the improved efficiency of cash and voucher assistance (CVA) using digital channels.[36] These approaches are often heavily reliant on connectivity, both for the responding agencies and the communities that they serve. Without connectivity, such efficiencies are not equally possible and the opportunity cost of failing to leverage digital tools can be significant. Similarly, the move towards self-referral and self-management of cases by aid users, which is being seen in some parts of the sector, becomes increasingly difficult when people cannot use connectivity services to access relevant platforms, minimising the efficiency gains.[37]

27 UNHCR. (2016). Connecting Refugees.
28 KII, several
29 KII, Humanitarian
30 Ibid.
31 Ibid.
32 KII, several
33 KII, Academic
34 KII, Humanitarian
35 Ibid.
36 Casswell, J. et al. (2019). Navigating the Shift to Digital Humanitarian Assistance: Lessons from the International Rescue Committee's Experience. GSMA.
37 KII, Humanitarian

1.4 Increased reliance on humanitarian assistance

Today, connectivity is enabling people to access public services, get an education, gain employment, run a business and relax, including in crisis-affected communities.[38] In ways other infrastructure cannot, connectivity allows people to access these services from a distance, opening opportunities for remote work[39] and education, selling goods to people in other parts of the world and accessing information at their fingertips. For example, GSMA research has found that small business owners in refugee camps use basic mobile phones for sales.[40]. Connectivity is also often perceived as vital to empowering refugees to be self-reliant.[41]

Mobile technology has played a transformational role in opening access to financial services, especially in rural areas that traditional banking infrastructure has not reached.[42] Mobile money technology was designed specifically with underserved rural communities in mind and has revolutionised the financial lives of millions of people around the world. While some mobile money functionality is available offline, it is severely limited without connectivity.

Multiple interviewees pointed out that a lack of connectivity can mean fewer economic opportunities and, therefore, limits people's potential to break cycles of aid dependency. This is not to say that crisis-affected communities in areas without network coverage cannot support themselves but, without connectivity, options are more limited.[43]

1.5 Poor economic development

Connectivity, especially mobile broadband,[44] has been shown to strengthen local economies and household spending power,[45] even in fragile and conflict-affected states.[46] Successful economies are more likely to create economic opportunities for people, and greater household spending power can prevent cycles of dependence on humanitarian assistance. While the presence of connectivity does not guarantee economic growth (there are several factors in crisis settings likely to curtail economic growth), the absence of it means that local economies will struggle to compete.

38 Ibid.
39 Ibid.
40 Casswell, J. (2019). The Digital Lives of Refugees. GSMA.
41 UNHCR. (2023). Digital Transformation Strategy 2022–2026: Strengthening protection, building self-reliance and optimizing delivery.
42 KII, Humanitarian
43 Ibid.
44 Connectivity from 3G onwards.
45 Bahia, K. et al. (2021). Mobile Broadband Internet, Poverty and Labor Outcomes in Tanzania. Policy Research Working Paper, No. 9749. World Bank.
46 World Bank. (2023). Digital Hotspots: Developing Digital Economies in a Context of Fragility, Conflict and Violence.

Information ecosystem

1.6 Not receiving vital information

Increasingly, digital channels and platform tools are becoming the default for users seeking up-to-date information and for organisations seeking to disseminate information quickly.[47] However, in communities where these are unavailable or challenging to access, people are at greater risk of missing out on vital and potentially life-saving information about a crisis, such as an early warning message about an imminent natural hazard. This can mean communities are unable to take appropriate actions to avoid physical harm, such as moving away from a dangerous area.[48]

Connectivity gaps can also affect people's ability to proactively seek information about a crisis through local media or social media.[49] This may make it more difficult to make important decisions about how to keep themselves and their families safe.

1.7 Fraud and disinformation

Situations in which people cannot easily fact check or validate information that is provided to them are fertile ground for misinformation and general and targeted disinformation. Multiple interviewees reported scams and fraud taking place in crisis settings with mobile coverage gaps. One example was cash programming, where people may impersonate humanitarian staff and ask someone for a payment to register them in a cash assistance programme. Without the means to verify this person's identity and not wanting to miss an opportunity, people may fall victim to fraud and financial harm.[50]

Similarly, there are growing concerns about crisis-affected people being targeted by human traffickers, especially those on the move. While these concerns vary depending on the setting (this is covered elsewhere in the report), in areas without mobile coverage, traffickers may lie about destinations or how easy a journey will be to traffic already potentially vulnerable people who cannot easily fact check this information.

Well-being

1.8 Poor psychosocial well-being

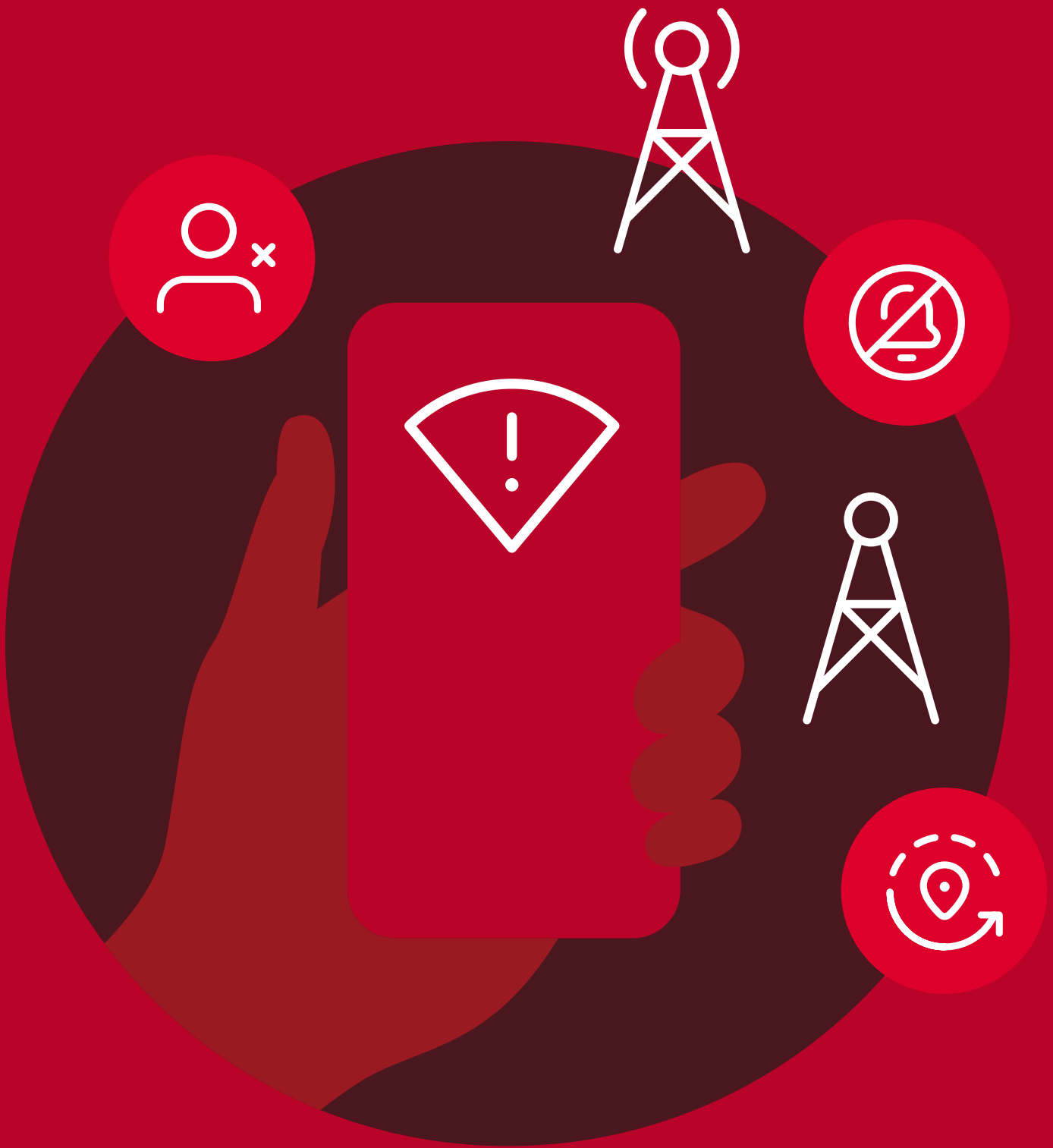
Interviewees reported that psychosocial well-being was at risk in areas without connectivity as it can make access to leisure activities, such as music, films, religion or games, more difficult.[51] A functional mobile network that enables people to make phone calls, text and message has clear benefits during a crisis.[52] In times of conflict, there is evidence to suggest that access to connectivity can be an important morale booster.

An important part of this is connecting with loved ones and a support network. Interviewees described the palpable sense of relief and reassurance among people in crisis-affected communities once a connection was established and they could confirm the safety of their loved ones.[53] A lack of connectivity can prevent information from being exchanged between loved ones, both day-to-day communication and the ability to let them know they are safe. This also affects people who live in connected areas but whose loved ones do not.[54]

47 Parsons, O. and Hamilton, Z. (2023). "Cell Broadcast for Early Warning Systems". GSMA.
48 KII, several
49 KII, Humanitarian
50 Ibid.
51 Ibid.
52 McDaid, C. (29 March 2022). "The Mobile Network Battlefield in Ukraine – Part 1". ENEA Insights.
53 KII, Humanitarian
54 Ibid.

02

Lost or limited connectivity



What does it mean to lose connectivity during a crisis?

Access to connectivity can often be lost or limited the moment a crisis occurs, with huge socio-economic and humanitarian implications. Arguably this is when connectivity is most critical – to contact loved ones, to find information and to call for help. **As our lives are lived more and more in digital spaces and we become more digitally dependent, the sudden loss of connectivity has greater and more complex implications than ever before.** For those who have become accustomed to, and reliant upon, digital services for information, finances and social connections, a sudden loss can have different and more pronounced effects than for those who live in low or no network settings and have not developed this same reliance.

There are a number of ways that connectivity can be lost or limited when crisis strikes, with different implications depending on the length of outages and why they have occurred. For example, service restriction orders (SROs), commonly known as internet shutdowns, use legal or regulatory measures to stop or slow access to some or all connectivity services. In some parts of the world, SROs have become increasingly common in recent years. Likewise, cyberattacks, physical attacks on infrastructure, fuel shortages and physical damage caused by natural hazards can all affect the ability of users to get online or access digital services.[55] This section outlines the primary causes of lost or limited connectivity within humanitarian settings and then examines the humanitarian risks this can create.

Service restriction orders

The use of government-mandated SROs has increased significantly in recent years. Access Now, a civil society organisation (CSO) that campaigns against the use of SROs, recorded 187 SROs in 2022 in 35 countries, more countries than ever before, and more than 1,000 since 2016.[56] The vast majority occurred in the past five years.[57] **The GSMA, as the representative body for MNOs, discourages the use of SROs and believes government authorities should only resort to using them in exceptional and pre-defined circumstances, and only if they are necessary and proportionate to specific and legitimate aims, consistent with international human rights laws and relevant local laws.**[58]

As SROs have proliferated, so have the types of restrictions. SROs can be limited to certain geographic areas within a country or be applied nationwide. Sometimes, MNOs receive SROs from authorities to restrict specific apps or content.[59] SROs can also restrict mobile broadband or data bandwidth to unusable speeds, also known as throttling.[60] The quality of the full network, including voice and SMS services, can be degraded.[61] Or, signal jamming can disrupt the connection between a device and its access point.

Likewise, there are a variety of ways that networks can be disrupted. In addition to SROs issued to MNOs, authorities can cut power, dismantle infrastructure, including cell towers and fibre optic cables, or disrupt network routers and domain name systems.[62] Some consider physical attacks on infrastructure (discussed later) as a form of service restriction. For the purposes of this analysis, these have been kept separate to illustrate the differences between connectivity restriction through legal or regulatory measures, including physically dismantling equipment, and the damage that happens through attacks in either symmetric or asymmetric warfare, usually by a foreign authority or non-state actor.

55 Tindall, T. (1 February 2022). "Blackout: understanding the internet shutdowns in Kazakhstan and Yemen". ODI; Feingold, S. (20 October 2022). "What happens when the internet shuts down?" World Economic Forum; GSMA. (2023). Mobile Telecommunications Security Landscape; KII, Technologist.

56 Access Now. (2022). Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022.

57 Guest, P. (26 April 2022). "In the Dark: Seven years, 60 countries, 935 internet shutdowns: How authoritarian regimes found an off switch for dissent". Rest of World.

58 GSMA. (2022). Mobile Policy Handbook: Consumer Protection.

59 Feingold, S. (20 October 2022). "What happens when the internet shuts down?" World Economic Forum.

60 GSMA. (2022). Mobile Policy Handbook: Consumer Protection; Guest, P. (26 April 2022). "In the Dark: Seven years, 60 countries, 935 internet shutdowns: How authoritarian regimes found an off switch for dissent". Rest of World; Feingold, S. (20 October 2022). "What happens when the internet shuts down?" World Economic Forum.

61 GSMA. (2022). Mobile Policy Handbook: Consumer Protection; Guest, P. (26 April 2022). "In the Dark: Seven years, 60 countries, 935 internet shutdowns: How authoritarian regimes found an off switch for dissent". Rest of World.

62 Feingold, S. (20 October 2022). "What happens when the internet shuts down?" World Economic Forum.

Physical attacks

Given the increasingly important role of connectivity and digital services in society, the physical infrastructure that supports it has increasingly become a target in conflict situations.[63] If attacked, physical network infrastructure presents a key vulnerability and can easily lead to the loss of connectivity for those who rely on it.

Cyberattacks

Depending on the type, cyberattacks can cause the loss of connectivity, including the inability to access digital services, or create new risks while connected.[64] In humanitarian settings, there are two primary types of malicious cyberoperations according to the ICRC: those seeking to obtain information and those seeking to disrupt services.[65] The CyberPeace Institute adds attacks for political or ideological purposes, such as those that aim to disrupt a particular operating environment.[66] In some cases, attacks that seek to disrupt services or are carried out for political purposes can cause the loss of connectivity.

Certain types of cyberattacks have a particular impact on users' ability to connect or access connectivity-enabled services. For example, malware can limit their ability to connect. Malware includes any kind of "malicious or intrusive software designed to damage, destroy or subvert computer systems." Likewise, distributed denial-of-service attacks, or DDOs, flood a network or service with excessive traffic with the intent to disrupt normal functioning. DDOs have been used to disrupt access to financial services, to information and even to humanitarian assistance.[67] Both state and non-state actors on both sides of recent conflicts have used cyberattacks.

Unintended loss of connectivity

There are several reasons connectivity can be lost during a humanitarian crisis without intent. Natural hazards, such as floods, earthquakes, storms and wildfires, can damage or destroy connectivity infrastructure or capabilities. Tonga, for example, was cut off completely from connectivity services following a massive earthquake that severed the single undersea cable that connects it.[68] With climate change, natural hazards will become more frequent and severe. The GSMA has done significant work in this area, including through its 2015 launch of the Humanitarian Connectivity Charter, helping MNOs to ensure their infrastructure is resilient and sufficient response protocols are in place.[69] Infrastructure can also be damaged for other reasons, including accidents.

It is also worth considering the extent to which other sources of connectivity disruption might be usefully included in this framework. For example, fuel shortages, supply chain disruptions, 2G/3G sunsets[70] and petty crime (including vandalism) can all cause a loss of connectivity, as found in recent GSMA research in Lebanon and Papua New Guinea.[71] Depending on the length of disruption, unintended connectivity losses can have the same impacts on users as intentional shutdowns and limitations. However, the cause and intent can also have an impact on the effects and types of possible responses.

63 CyberPeace Institute. (2022). "Guerre en Ukraine : la lutte for le controle du reseau informative et son impact sur les civils"; KII, Humanitarian
64 GSMA. (2023). Mobile Telecommunications Security Landscape.
65 Macak, K. and Vignato, M. (25 April 2023). "Civilianisation of Digital Operations: A Risky Trend". Lawfare.
66 Stakeholder interview, humanitarian organisation
67 CyberPeace Institute. (2023). "Cyber Attacks in Times of Conflict."
68 Vincent, J. (19 January 2022). "A lone undersea cable connected Tonga to the world – a volcanic eruption broke it". The Verge.
69 Hamilton, Z. and Tillekeratne, D. (2020). Building a Resilient Industry: How Mobile Network Operators Prepare for and Respond to Natural Disasters.
70 While network sunsets are not in themselves accidental, they are included here as they do not come with a specific or malicious intent to deny people access to connectivity.
71 GSMA and UNHCR. (2022). The Digital Worlds of Displacement-Affected Communities.

Humanitarian implications

Regardless of the cause, the humanitarian risks and implications of lost or limited connectivity during a crisis can vary, from the intent of the actors involved to the duration. If connectivity is lost for a long period, the risks can switch from the ones outlined in this chapter to those associated with a complete lack of connectivity, as outlined in the previous chapter. The type of crisis is also important and influences what type of response is possible. For example, it may be easier to repair a tower that has been damaged by a storm than one that has been intentionally damaged in a conflict setting, potentially reducing the humanitarian implications.

The following section outlines the primary humanitarian implications of lost or limited connectivity during a crisis.

Protection

2.1 Limited connectivity as a human rights violation

Cutting off connectivity can be considered, in many cases, to be a violation of human rights. In 2016, the United Nations recognised the importance of internet access to human rights.[72] Connectivity is also a key enabler of other basic human rights, including the right to freedom of expression, the right to assembly and the right to life.[73] Restricting people's access to connectivity can be a way to restrict the free flow of information or hinder a political opponent's ability to assemble.[74]

Additionally, and as discussed in chapter 1, limiting access to connectivity can also limit people's ability to report on secondary human rights violations. Connectivity and mobile technology have come to play an important role in helping citizens document and share information with the outside world on current realities.

Humanitarian aid and coordination

2.2 Barriers to humanitarian aid and programming

The sudden loss or limitation of connectivity can prevent humanitarian assistance from reaching intended recipients or limit the ability of humanitarian organisations to operate in an area at all. When connectivity is lost, especially when operations rely on connectivity services to coordinate, humanitarian organisations often cannot work safely.[75] This applies to digital humanitarian programming, such as supplying information via social media or cash programming using mobile money, but also to the ability of humanitarian organisations to coordinate internally and maintain contact with staff. In this way, service restriction acts like a physical access restriction, limiting and curtailing the delivery of aid.

Related to this is the impact on humanitarian organisations' ability to coordinate, as mentioned in 1.3, Barriers to efficient humanitarian coordination. Without connectivity, it is challenging to understand the crisis at hand – the situation, the scale and the humanitarian needs – and to coordinate activities. These challenges risk leaving affected populations unable to access the services they need and are entitled to.

72 Howell, C. and West, D. (7 November 2016). "The internet as a human right." TechTank. Brookings.
73 GSMA. (2022). Mobile Policy Handbook: Consumer Protection.
74 Feingold, S. (20 October 2022). "What happens when the internet shuts down?". World Economic Forum.
75 KII, several

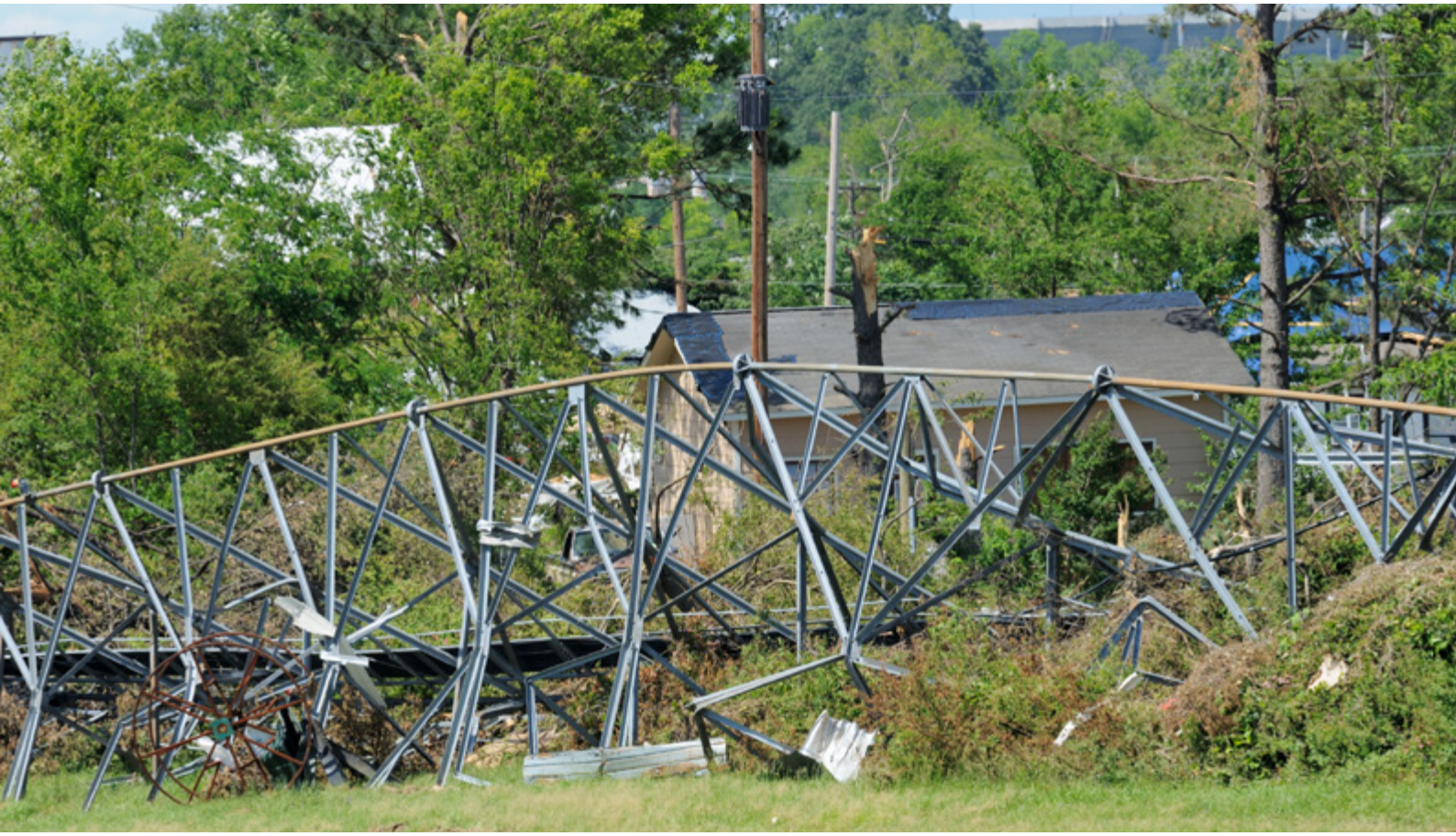
Information ecosystem

2.3 Disruption of access to timely and accurate information

Limited access to connectivity can have profound implications for the information ecosystem during crises. One of the main things people use connectivity for is to find information, and this becomes especially important for people navigating crisis when accurate information can be matter of life or death.[76] This includes information that humanitarian organisations are actively seeking to provide – on available services, safe shelter and the current situation – and the information ecosystem more broadly. The risks of limited access to connectivity (see 1.6 Not receiving vital information) include the ability to send or receive early warning messages and to take the steps they need to minimise risk to themselves and their loved ones.

2.4 Misinformation and disinformation

Without the ability to seek and verify information online or through social networks (see 1.7 Fraud and Disinformation), information vacuums can form, leading to rumours and misinformation.[77] In Lebanon, for example, when a massive explosion devastated the Port of Beirut in 2020, communication channels were disrupted. As a result, rumours spread that the explosion was an attack.[78] Likewise, there may be increased risks of bad actors intentionally taking advantage of the information vacuum. During connectivity outages in Latin America, UNHCR noted an increase in fraudulent organisations posing as humanitarian service providers and extracting money from affected populations to ostensibly access services.[79]



76 KII, Humanitarian
77 Ibid.
78 Ibid.
79 KII, Humanitarian

Autonomy

2.5 Disruption of social networks and community resilience mechanisms[80]

In most crises, first responders are communities themselves. Disruptions to connectivity, therefore, risk disrupting social networks and community resilience mechanisms. For example, people may not be able to use the services on which they have come to rely, like accessing remittances from friends and family, contacting loved ones to let them know they are safe or calling to ask for help.[81] Many interviewees cited the risk of not being able to find loved ones and the increased risk of isolation and long-term displacement this can create.[82]

2.6 Economic impacts

Limited or regular loss of connectivity can have profound effects on macroeconomic stability, as businesses are not able to function as usual. A UN study found that between 2019 and 2021, SROs cost the world's 46 affected countries $20.5 billion.[83] The direct loss of business profits during a government-mandated SRO is not the only cost; the climate of instability created by shutdowns can also have lasting impacts on investment in the country, on the emigration of young people and on tourism.[84] In the long term, these macroeconomic destabilising effects can drive food insecurity, create more humanitarian need and reduce the resilience of a country and its people.

2.7 Disruption of the normal functioning of services

In terms of people's daily lives, disruptions to connectivity and subsequent disruptions to the regular functioning of services can also have massive humanitarian implications affecting nearly every aspect of life, from healthcare to livelihoods to health. For example, government mandated SROs have been know to limit the ability of healthcare professionals to access up-to-date information on conditions and treatments.[85]

Well-being

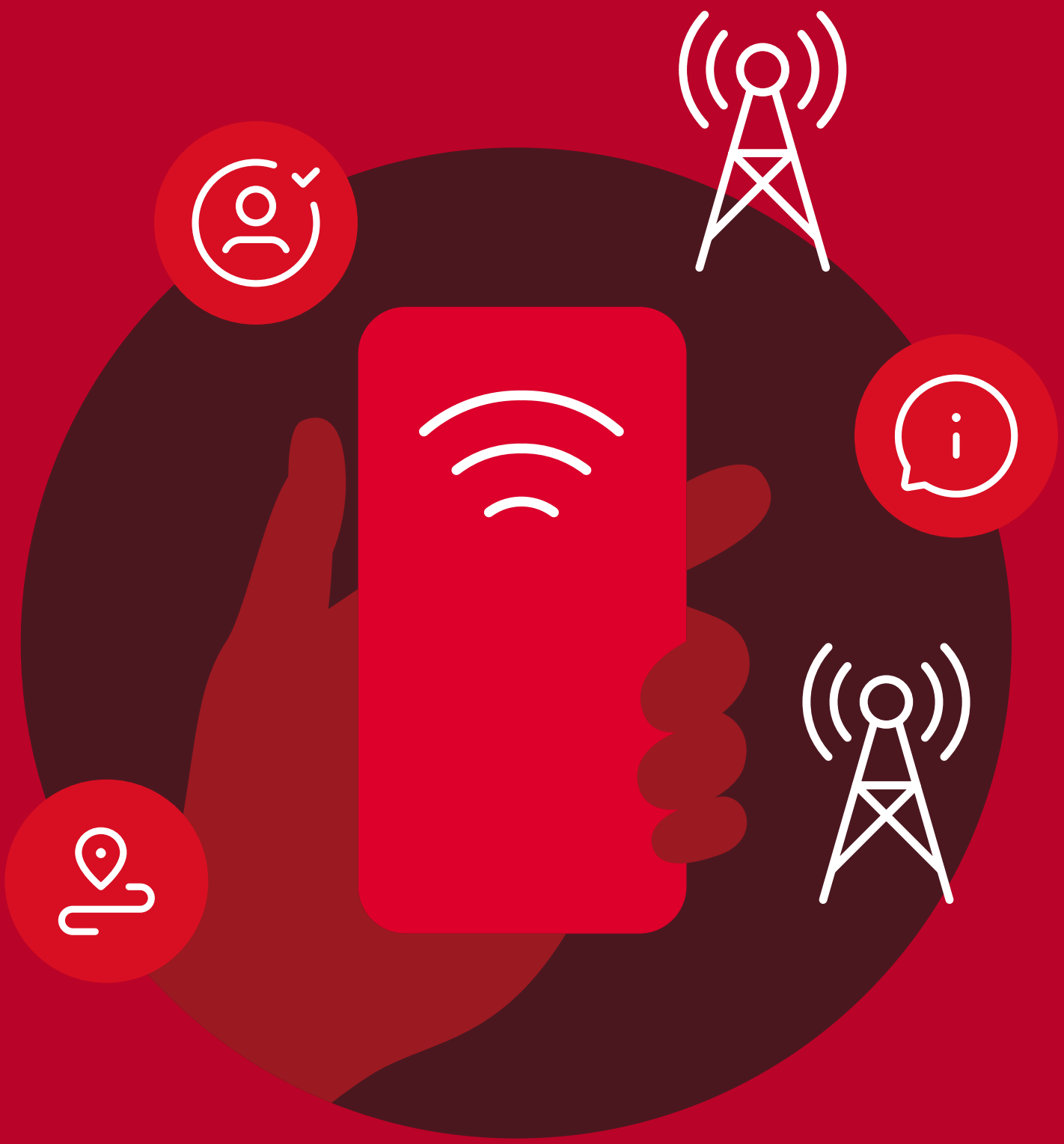
2.8 Psychosocial well-being

Connectivity also plays an important psychosocial role. When it is lost suddenly, the stress of not being able to access information, services or loved ones should not be underestimated.[86] Additionally, having connectivity and a sense of control is extremely important to human dignity. For people already experiencing the stress of sudden violence, crisis or disaster, the loss of connectivity can exacerbate this stress.[87] When connectivity is targeted intentionally, this may contribute even more to psychological stress.

80 Jaspers, S., Murdoch, C. and Majid, N. (2022). Digital feast and famine: Digital technologies and humanitarian law in food security, starvation and famine risk.
81 KII, Humanitarian
82 KII, several
83 Feingold, S. (20 October 2022). "What happens when the internet shuts down?". World Economic Forum.
84 Guest, P. (26 April 2022). "In the Dark: Seven years, 60 countries, 935 internet shutdowns: How authoritarian regimes found an off switch for dissent". Rest of World.
85 Sirnate, V. and Jain G. (3 April 2023). "Democracy is dying in digital darkness." APC.
86 KII, Humanitarian actor
87 KII, Humanitarian

03

Stable connectivity: connected crises



What does it mean to have a mobile connection when a crisis strikes? How is connectivity changing the nature of crises?

In 2022, the GSMA estimated that 4.6 billion people, 57% of the global population, were using mobile internet services and 95% lived within the footprint of a mobile network. In the least developed countries (LDCs), one in four people are now using mobile internet. These numbers continue to grow year on year, although the rate of growth is slowing.[88] In many places, connectivity already plays a role in the lives of crisis-affected communities, demanding continued and focused attention.[89]

The potential benefits of connectivity for crisis-affected communities are numerous and sometimes transformational, yet it is not risk free. **In an increasingly digital world where more and more of the human experience takes place online, connectivity can exacerbate existing risks and introduce new ones, leading to ever-changing challenges for people affected by crisis and humanitarian responders.** This can include risks related directly to connectivity and digital exclusion, but can extend far beyond.[90]

Connectivity-related risks, for example, include the ways in which historically marginalised groups, who are traditionally less likely to be online, find it more difficult to access services as humanitarian assistance shifts to digital channels. For example, in Bidi Bidi Refugee Settlement in Uganda, women were found to be 47% less likely to own a mobile phone than men, and people with disabilities were 10% less likely to own one than people without disabilities.[91] This connectivity access gap can not only have long-term impacts on the ability of marginalised populations to access information and services, but also on their overall well-being. Likewise, a World Bank and GSMA study found that mobile connectivity had significant positive impacts on household well-being in Nigeria, which were not felt equally across age groups and gender lines. This unequal access can diminish the potential long-term benefits of being connected,[92] and illustrates the risks of entrenching historical marginalisation through digital exclusion.

In chapter 4, more attention will be paid to the ways in which digital exclusion and other factors can affect how users experience connectivity risks. However, for the rest of this chapter, we examine the risks that come from being digitally connected, assuming crisis-affected communities have the ability to connect.

Technology-facilitated harm includes harm faced online or in digital spaces, as well as offline harms that are rooted in, or amplified by, being connected. For example, just as protection risks exist in the physical world, so too do risks of protection in the digital world, like verbal harassment, surveillance or assault on a social media platform.[93] These online risks can also translate into offline risks, for example, online harassment can extend to physical harassment or targeting of individuals in the "real world". These risks are often intertwined and impossible to disaggregate.

As technology continues to advance, these challenges will likely become more complex and unavoidable. New innovations, like deep fakes, will create new humanitarian challenges for crisis-affected communities that are navigating information ecosystems and will likely be weaponised against responding agencies. It will be important to monitor technological advances to understand and address emerging risks.

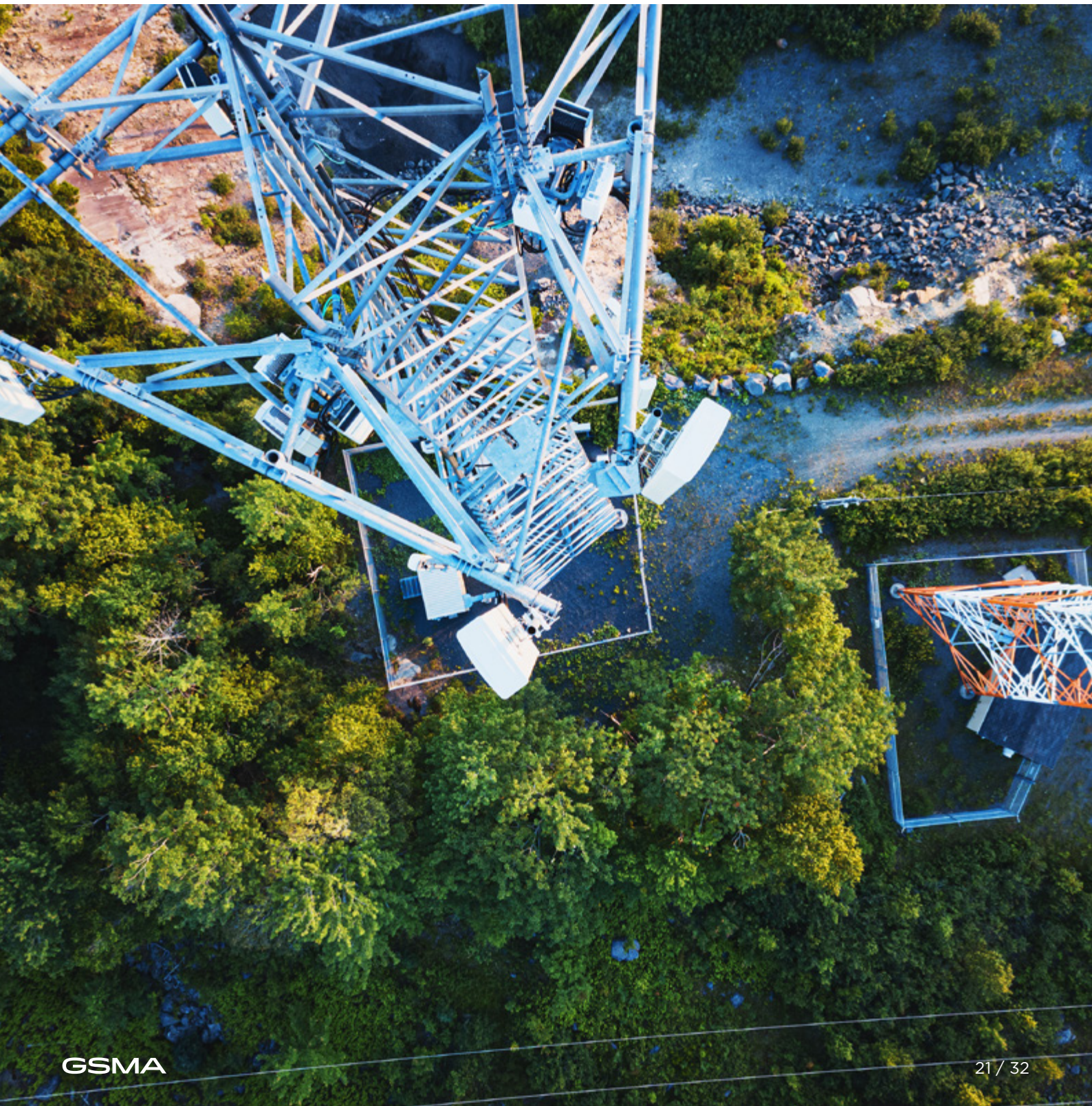
Despite these challenges, it is the opinion of the GSMA that these risks should not be used by the humanitarian community as a justification for not giving people access to potentially life-saving digital services. Instead, acknowledging these risks is the first step in enabling the humanitarian community, including technology providers and private sector partners, to take appropriate action to mitigate and respond to them.

88 GSMA. (2023). The State of Mobile Internet Connectivity Report 2023.
89 KII, Humanitarian actor
90 Ibid.
91 Casswell, J. (2019). The Digital Lives of Refugees. GSMA and UNHCR.
92 World Bank and GSMA. (2020). The Welfare Effects of Mobile Broadband Internet: Evidence from Nigeria (English).
93 Internews. (2023). "Safe Sisters".

Humanitarian implications

While most interviewees emphasised that the opportunities of connectivity largely outweigh the risks, it is essential to articulate and understand the humanitarian implications of being connected during a crisis. The risks to which users are exposed can vary depending on many factors, especially their intersectional identities. Groups that are marginalised in the physical world, whether that be based on gender identity, ethnic identity or political affiliation, for example, are also likely to face greater risks in the digital world.

However, perhaps one of the greatest risk factors within a connectivity context is digital literacy. For users who are becoming connected for the first time, especially vulnerable or marginalised groups, digital literacy and awareness of digital risks tend to be lower and present acute challenges. Greater awareness of these risks, and how to mitigate them, can lessen potential harms but will not usually eliminate them. More information on the impact of digital literacy can be found in chapter 4.



Protection

3.1 Harassment, violence and hate speech

Harm that is perpetrated online can also have offline implications, such as online gender-based violence (GBV), hate speech or verbal harassment or assault. In 2020, UNHCR Ecuador found that refugee women and LGBTQI+ people were particularly at risk of online gender-based violence (GBV), including unsolicited photos and threats.[94]

When working with populations who may have fled their homes due to their identities or political affiliations, it is vital to understand the risks of online targeting. Hugo Slim, in his book, *Solferino 21: Warfare, Civilians and Humanitarians in the 21st Century*, suggested that in a new era of digital civilians, people are being forced to flee not only in the physical world but also in the digital world.[95] In recent research conducted with Syrian refugees in northern Lebanon, the GSMA and UNHCR found that people were wary of going online or using social media, both because of concerns about surveillance and encountering hate speech and online abuse.[96]

3.2 Narratives can create hostility and exacerbate conflict

Misinformation, disinformation and hate speech (MDH), including those intentionally spread through cyberinfluence operations, can cause multiple types of harm. First, they can create a challenging information landscape for people in crisis to navigate (see 3.6 Murky information ecosystems). Narratives that are spread online can create hostility, undermine truth and exacerbate conflict, whether intentionally or otherwise. For example, misleading information or propaganda about the "enemy" on social media can fuel conflict or promote certain narratives about who is responsible for a crisis. Members of crisis-affected communities can both participate in MDH, knowingly or not, and be the targets of it.[97]

If not handled with care, this hostility can affect the delivery of humanitarian assistance or stoke tensions between displaced populations and the communities that host them.[98] For example, in Lebanon, a humanitarian agency had to postpone a planned distribution due to misinformation on YouTube that was deemed likely to escalate into violence. Similarly, UNHCR found that refugees and migrants in Chile were targeted with xenophobic hate speech online by local nationalist groups then physically attacked them and people in their neighbourhoods.[99]

Social media, in particular, has amplified the spread of MDH as the algorithms can boost volatile content. However, MDH can spread on many channels, including encrypted channels like WhatsApp, making it challenging to monitor and address.[100]

94 KII, Humanitarian sector
95 Slim, H. (2022). Solferino 21: Warfare, Civilians and Humanitarians in the 21st Century.
96 GSMA and UNHCR. (2022). The Digital Worlds of Displacement-Affected Communities.
97 Slim, H. (2022). Solferino 21: Warfare, Civilians and Humanitarians in the 21st Century.
98 CDAC Network. (13 June 2023). "The state of communication, community engagement and accountability across the Ukraine response and an overview of key activities".
99 KI, Humanitarian; France 24. (27 September 2021). "UN concerned about 'xenophobia' against migrants in Chile".
100 KII, Humanitarian

3.3 Risk of targeting and surveillance

Online information may also be used to track, monitor and target people physically. Personally identifiable information such as phone numbers, IMEI numbers and IP addresses, as well as location data, can be used to target individuals or communities.[101] Use of digital services or the simple act of being online can create new data sets around individuals that can lead to offline harm for certain groups,[102] and nefarious technologies like malware can be used to extract user data or contacts.[103] Again, these risks are more acute for marginalised groups or people fleeing persecution. In the Americas, interviewees noted that refugees were often hesitant to post on social media publicly or use their real names.[104]

Malevolent actors who gain access to user locations, financial information, personal contacts, online activities and other data, can pose a humanitarian risk. State or non-state actors can infiltrate systems to extract information for surveillance or intelligence purposes and to target individuals and groups.[105] This can then create new risks, such as exacerbating a conflict or hindering the ability of humanitarian agencies to provide services.

3.4 Trafficking risks

It remains an open question whether increased access to information via connectivity helps people find safer ways to move across borders; the risk of exposure to traffickers can happen both online and offline.[106] However, traffickers are known to use online spaces to recruit victims and continue to exploit them.[107] For example, in 2019 and 2020 when many Venezuelans were fleeing the country, people turned to Facebook groups to find information. Many human traffickers spent time in these groups, providing inaccurate information, offering to support people on their journeys for an exorbitant price or abandoning people en route once they had their fee.[108] It has also been reported that Ukrainian women have been targeted online with false housing and job offers in neighbouring countries.[109]

3.5 Scams and fraud

While the risk of scams or being taken advantage of through digital channels is not unique to humanitarian contexts, the consequences can be greater. For example, if a person loses some or all of their cash assistance to a scam, they no longer have the support designed to meet pressing needs.

Many types of fraud have been reportedly targeted specifically at crisis-affected communities. They range from traditional financial scams, fake prizes, false job opportunities, all the way to imitations of humanitarian services such as fake offers of resettlement.[110] UNHCR has found their logo being used in Facebook groups offering false humanitarian services, either at a cost or to steal users' data.[111] In Papua New Guinea, 7% of refugees residing in Iowara said they had been exposed to a scam, 38% of whom reported experiencing harm.[112] More sophisticated scams include stealing people's personal and financial data through cyberattacks and malware.[113]

Especially when introducing users to digital services and tools for the first time, the risks of scams or being taken advantage of are higher. When humanitarian organisations and their partners introduce digital tools, there is a question as to their responsibilities in helping to mitigate some of these risks and educate people to recognise and mitigate potential harms.

101 Slim, H. (2022). Solferino 21: Warfare, Civilians and Humanitarians in the 21st Century; KII, Humanitarian actor
102 KII, Humanitarian
103 KII, Private sector
104 KII, several
105 CyberPeace Institute. (2023). "Cyber Attacks in Times of Conflict".
106 KII, Humanitarian
107 Conference of the Parties to the United Nations Convention against Transnational Organized Crime. (2021). Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons.
108 KII, Humanitarian
109 Ibid.
110 Ibid.
111 Ibid.
112 GSMA. (2022). Iowara, Papua New Guinea: The Digital Worlds of West Papuan Refugees.
113 KII, Private sector

Information ecosystem

3.6 Murky information ecosystems

During a crisis, the ability to find accurate and relevant information quickly is vital. While connectivity has increased access to information, it has also made the information landscape far more challenging to navigate. Sifting through vast amounts of information is a huge challenge for many people in crisis. A study by the CDAC Network found that 57% of Ukrainian refugees in Hungary reported not knowing where to look for the information they needed, and 29% did not trust the information when they did find it. Refugees in Moldova reported similar challenges navigating social media, saying they were overloaded with information.[114]

MDH, as discussed earlier, can muddy the waters as rumours, propaganda and misinformation spread and are challenging to differentiate from accurate information. Trustworthy information is also difficult to find when information is designed poorly, not easily accessible or not tailored to the local context. When provided by a humanitarian organisation, this type of poorly designed information can sow mistrust. Digital literacy and the ability to triangulate and verify the accuracy of information sources are key for users to navigate risks.

Humanitarian aid and coordination

3.7 Remote humanitarian assistance

As humanitarian information and services digitalise, there are concerns this is creating distance between responders and the people they serve.[115] For some, digital humanitarian services are a positive development, such as proponents of "self-service" portals where people can register for help and even receive it remotely, sometimes with no face-to-face interaction at any point.[116] For others, this distance is considered a risk, as it can make it more difficult for humanitarian responders to understand or empathise with crisis-affected communities and potentially lead to more technocratic responses, devoid of individual accountability.[117] Digital channels also run the risk of making people less comfortable to approach humanitarian organisations and access services, since physical distance can foster mistrust among some groups.[118] However, trust in digital services is clearly context-specific, as interviewees noted that, for some groups, digital channels have enhanced trust and feelings of "closeness", such as among LGBTQI Venezuelan refugees in Colombia.[119]

3.8 Difficulty keeping in touch with service users

Reliance on connectivity for engagement and the need to have up-to-date phone numbers or potentially email addresses, can make it difficult to maintain contact with users of humanitarian services. In parts of the world where it is common to use multiple SIM cards or swap SIMs to get the best deal, contact with users can be lost until they make contact again. This can make it difficult, if not impossible, to communicate updates or provide humanitarian services and information, especially when people are on the move and their location is not easy to pinpoint.

114 CDAC. (13 June 2023). "The state of communication, community engagement and accountability across the Ukraine response and an overview of key activities".
115 Bryant, J. et al. (2020). Bridging humanitarian digital divides during Covid-19. ODI.
116 KII, several
117 KII, Academic
118 KII, Humanitarian
119 Internews. (2021). On the move during the COVID-19 pandemic: Information, trust and influence among Venezuelans in Nariño, Colombia.

04

Human and structural factors affecting connectivity

This paper's central analysis knowingly oversimplifies how connectivity works, both technologically and socially. While this is useful in broadly articulating the humanitarian implications of connectivity, both technological and social, it is important to also examine the human and structural factors that shape access to connectivity and the lived online experiences of crisis-affected communities.

Staying intentionally unconnected

Many people choose not to be connected, regardless of the availability or strength of networks in their area. Individuals who are concerned about being identified or located may choose to minimise connectivity or keep a low profile online. Some may not want their presence in a particular location known, for example, to claim asylum in another country later in their journey, or to avoid harassment or physical targeting.[120] Negative experiences online, like exposure to hate speech or harassment or distrust of technology, can also lead some users to avoid using digital services.[121]

Regardless of the availability of a network, an individual who chooses to not be connected will likely experience risks similar to those described in settings with no or lost connectivity. Similarly, a person who uses one digital service while avoiding others may encounter a range of connectivity risks and greater opportunity for digital exclusion.

Digital exclusion

There is a large and growing body of evidence that, in much of the world, women,[122] people with disabilities,[123] minority language speakers and other groups, are disproportionately excluded from digital access and the benefits of mobile connectivity. Similar trends have been seen in several humanitarian contexts.[124] The driving factors of digital exclusion vary, and often include a lack of digital skills, levels of functional literacy, language proficiency, ability to pay, safety and security, perceived relevance and social norms.[125]

For example, gender norms in some parts of the world mean that many women are unable to use digital services regularly and independently, due to male family members being "gatekeepers" of mobile phone use in their household.[126] Likewise, minority language speakers may be unable to use digital services if those services are not available in a language in which they are proficient, and people with limited financial resources may not be able to afford a mobile phone, to charge a handset or to buy airtime or internet data.[127]

When these factors are combined, digitally excluded individuals may live in settings with fully functional networks but remain unable to access connectivity in a meaningful way. This means their experiences are likely to resemble those of people living without connectivity, regardless of network availability.

120 KII, Humanitarian
121 KII, Technologist; GSMA and UNHCR. (2022). The Digital Worlds of Displacement-Affected Communities.
122 GSMA. (2023). The Mobile Gender Gap Report 2023.
123 GSMA. (2021). The Mobile Disability Gap Report 2021.
124 Casswell, J. (2019). The Digital Lives of Refugees. GSMA;GSMA and UNHCR. (2023). The Digital Worlds of Displacement-Affected Communities; Bryant, J. (2022). Digital technologies and inclusion in humanitarian response. ODI.
125 GSMA. (2023). The State of Mobile Internet Connectivity Report 2023.
126 KII, Humanitarian; GSMA. (2023). The Mobile Gender Gap Report 2023; Butler, C. and Shanahan, M. (2020). "Does just being a woman reduce the likelihood of using mobile?" GSMA Mobile for Development Blog.
127 Casswell, J. (2019). The Digital Lives of Refugees. GSMA.

Digital skills and capacity

Although inherently linked to digital exclusion, digital skills and capacity can have broad and nuanced impacts on the connectivity risks and opportunity costs for individuals during periods of crisis. A lack of critical digital skills and capacity can prevent some users from accessing digital services, manifesting in the same way as other types of digital exclusion and individuals experiencing the same risks that are associated with not being connected.[128]

At the same time, individuals without the requisite digital skills and capacity can be exposed to greater risks once they are connected because they may be unaware of the risks or how to manage them. For example, people with less experience with digital services or fewer digital skills, such as children or marginalised groups, may be at greater risk of not recognising scams or disinformation and, therefore, of being harmed by them.

People on the move

There is a somewhat implied assumption in this report that people affected by crisis stay in the same place and experience a static state of connectivity. However, as frequently discussed in interviews for this report, human mobility is common and widespread. People who are forcibly displaced, migrating or living a nomadic lifestyle may move through a variety of connectivity scenarios, losing connectivity as they enter one area and then regaining it, intermittently or fully, in others.

For example, interviewees cited the experience of many Syrian refugees, who may cross five countries from their point of departure to their destination, encountering various connectivity scenarios along the way. Each new setting presented new challenges, constraints and regulatory environments, with know-your-customer (KYC) requirements, roaming agreements and airtime costs all affecting their ability to connect and requiring different remedies or workarounds.[129]

Interviewees also highlighted examples of communities that were displaced from areas with strong connectivity to areas with no or low levels of connectivity. For example, from parts of Somalia with high levels of digitalisation, to more rural areas of Ethiopia where connectivity was much more limited. The result was both frustration (in many ways resembling the risks outlined in sections 2.5–2.10) and creative uses of technology. People found ways around their lack of connectivity, such as using Bluetooth to share content.[130] Likewise, when people fleeing Sudan crossed into Egypt, many lost connectivity services at and around the border, exposing them to the risks outlined in sections 2.1–2.10.

Similarly, individuals who have lived without mobile network coverage in their daily lives may travel to areas with coverage and, over the course of a single day, may be exposed to risks in all three categories of this analysis. Some interviewees also discussed the potential of connectivity to drive and compound the experience of displacement, although this remains largely anecdotal and hypothetical and will require further study.

128 Martin, A. (2021). Connecting with Confidence: Managing Digital Risks to Refugee Connectivity. UNHCR.
129 KII, Technologist
130 KII, Humanitarian

Impacts on users in other locations

While perhaps not central to concepts of network access, when considering communication functions of connectivity, it can be important for humanitarians to consider the impacts on those outside a humanitarian context who are trying to reach people within it.

Even if one party is in a connected setting, if they are trying to get in touch with someone in an area that is uncovered or has lost connectivity, the experience is effectively the same as having no connectivity, which can lead to significant psychological stress.

Politics and regulation

Political and regulatory landscapes can affect how crisis-affected communities experience connectivity. For example, the ease with which SROs can be implemented or the impact of KYC requirements and connectivity-related taxes on their ability to take advantage of connectivity services. In many jurisdictions, refugees are unable to access SIM cards in their own name, limiting their ability to access connectivity services and rendering them unconnected, regardless of local infrastructure.

Trust

Much of the analysis in this report relates to the ability to find, validate and engage with information. An examination of the information ecosystem and its inherent risks is incomplete without considering the trust people have in the information they receive and where it comes from, whether government, civil society or humanitarian organisations. Given the overwhelming amount of information available, building trust in humanitarian messaging is a complex task. People will only accept information from a trusted source, and in scenarios where they do not have one, people will be less able to overcome this risk.[131] Humanitarian organisations may need to consider the challenges of this new reality and how the information they provide exists within this wider context. Broadcasting accurate information in one direction may no longer be sufficient.

131 Internews. (2023). The Trust Framework.

Conclusion

The digital transformation of the humanitarian sector will continue to grow. This shift will continue to bring new opportunities for humanitarian actors to meet the needs of more people, more quickly, more efficiently and tailored to individuals. However, the sector needs to grapple with, and mitigate the risks and opportunity-costs in this analysis with ever increasing urgency. Analyses of this kind will need to be updated regularly as technology advances and introduces new issues and risks.

There will likely be a need to form collaborative, cross-sectoral coalitions to advocate, drive change and galvanise action to close coverage gaps. For example, the GSMA is collaborating with UNHCR and the International Telecommunication Union (ITU) on a Refugee Connectivity Mega Pledge, which aims to accelerate the expansion of connectivity services to refugees currently outside mobile network coverage. The expansion of networks at scale will likely remain market-led, fuelled by aggregated demand and driven by the private sector. **However, if humanitarian and development actors neglect the issue and humanitarian coverage gaps are allowed to continue to exist, the risks to crisis-affected communities could become even more severe and may even come into contention with the humanitarian principles of impartiality and do no harm.**

As crisis-affected communities and humanitarian responders become increasingly dependent on connectivity, the risks will be greater when it is lost, whether intentionally or otherwise. As natural hazards become more frequent and severe in the climate crisis, and if service restriction orders increase in line with recent trends, it is likely that crisis-affected communities and those seeking to help them will need to mitigate and overcome these risks more regularly. **This will likely require effective cross-sectoral advocacy at national and international levels, alongside work to secure, reinforce, and protect connectivity networks.**

As we have emphasised throughout this report, the availability and accessibility of connectivity networks is not a risk-free panacea. Crisis-affected communities will continue to face the risks outlined in this analysis and others,[132] and are virtually guaranteed to face new and heightened risks as technology advances. **Stakeholders therefore need to stay vigilant, monitor advances in technology and listen and adapt to the feedback and concerns of people living in crisis.**

Importantly, marginalised groups are both more likely to be digitally excluded even when they have network coverage and to face additional risks once they are connected. These groups must be considered at every stage of digital humanitarian programming to ensure an inclusive and safe digital ecosystem.

It will also be essential to consider the respective responsibilities of the humanitarian and private sectors in connecting crisis-affected communities. For many, the greatest benefit of connecting communities is the autonomy it provides, removing some of the control over assistance by the international humanitarian system and enabling people to reach out and ask for it. Connectivity also reduces the gatekeeping of vital information and enables people to find it for themselves.

It will be important to balance the humanitarian obligation to protect and ensure people do not experience harm, with a humanitarian system that does not approach the digital lives of people in ways that are paternalistic or condescending. **Meanwhile, the wider humanitarian community must work together to ensure humanitarian organisations have the skills to manage an increasingly digitised sector, including strong data protection practices, system redundancies and offline alternatives.**

With all this in mind, it is essential that stakeholders continue to gather evidence and work together in broad coalitions to maximise the opportunities and minimise the risks of connectivity in times of crisis. This preliminary analysis is a starting point – to document and articulate what does, can or may create new risks or opportunity costs for crisis-affected communities – and hopefully invites further discussion and action. The GSMA remains committed to working with a range of stakeholders to address these issues through research, policy, programming, and innovative funding.

132 ICRC. (2023). Protecting Civilians Against Digital Threats During Armed Conflict.

References

Access Now. (2022). *Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022.*

AP. (20 September 2023). "Flood rescue teams in Derna set back by communications outage", *The Guardian.*

Bahia, K. et al. (2021). *Mobile Broadband Internet, Poverty and Labor Outcomes in Tanzania.* Policy Research Working Paper; No. 9749. World Bank. Washington, DC.

Bryant, J. (2022). *Digital technologies and inclusion in humanitarian response.* ODI.

Bryant, J. et al. (2020). *Bridging humanitarian digital divides during Covid-19.* ODI.

Butler, C. and Shanahan, M. (2020). "Does just being a woman reduce the likelihood of using mobile?" *GSMA Mobile for Development Blog.*

Casswell, J. (2019). *The Digital Lives of Refugees.* GSMA and UNHCR.

Casswell, J. et al. (2019). *Navigating the Shift to Digital Humanitarian Assistance: Lessons from the International Rescue Committee's Experience.* GSMA.

CDAC. (13 June 2023). "The state of communication, community engagement and accountability across the Ukraine response and an overview of key activities".

CyberPeace Institute. (2022). "Guerre en Ukraine : la lutte for le controle du reseau informative et son impact sur les civils".

CyberPeace Institute. (2023). "Cyber Attacks in Times of Conflict."

Development Initiatives. (2023). *Global Humanitarian Assistance Report 2023.*

Downer, M. (2019). *Bridging the mobile gender gap for refugees.* GSMA.

Feingold, S. (20 October 2022). "What happens when the internet shuts down?" World Economic Forum.

France 24. (27 September 2021). "UN concerned about 'xenophobia' against migrants in Chile".

GSMA. (2021). *The Mobile Disability Gap Report 2021.*

GSMA. (2022). *Iowara, Papua New Guinea: The Digital Worlds of West Papuan Refugees.*

GSMA. (2022). *Mobile Policy Handbook: Consumer Protection.*

GSMA. (2023). *Mobile Telecommunications Security Landscape.*

GSMA. (2023). *The Mobile Gender Gap Report 2023.*

GSMA. (2023). *The State of Mobile Internet Connectivity 2023.*

GSMA and UNHCR. (2022). *The Digital Worlds of Displacement-Affected Communities.*

Guest, P. (2022). "In the Dark: Seven years, 60 countries, 935 internet shutdowns: How authoritarian regimes found an off switch for dissent". Rest of World.

Hamilton, Z. and Tillekeratne, D. (2020). *Building a Resilient Industry: How Mobile Network Operators Prepare for and Respond to Natural Disasters.*

Howell, C. and West, D. (7 November 2016). "The internet as a human right." *TechTank.* Brookings.

ICRC. (2023). *Protecting Civilians Against Digital Threats During Armed Conflict.*

Internal Displacement Monitoring Centre. (2022). *Global Internal Displacement Database.*

Internews. (2021). *On the move during the COVID-19 Pandemic: Information, trust and influence among Venezuelans in Narino, Colombia.*

Internews. (2023). *Information and Risks: A Protection Approach to Information Ecosystems.*

Internews. (2023). "Safe Sisters".

Internews. (2023). *The Trust Framework.*

ITU. (2020). *The Last-mile Internet Connectivity Solutions Guide: Sustainable Connectivity Options for Unconnected Sites.*

Jaspers, S., Murdoch, C. and Majid, N. (2022). *Digital feast and famine: Digital technologies and humanitarian law in food security, starvation and famine risk.*

Lough, O. et al. (2023). *Beyond survival: exploring wellbeing in humanitarian action.* ODI

Mačák, K. (2023). "Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield". *International Review of the Red Cross.*

Macak, K. and Vignato, M. (25 April 2023). "Civilianisation of Digital Operations: A Risky Trend". *Lawfare.*

Martin, A. (2021). *Connecting with Confidence: Managing Digital Risks to Refugee Connectivity.* UNHCR.

McDaid, C. (29 March 2022). "The Mobile Network Battlefield in Ukraine – Part 1". *ENEA Insights.*

Notre Dame Global Adaptation Initiative. (2023). *ND-GAIN Matrix.*

Parsons, O. and Hamilton, Z. (2023). *Cell Broadcast for Early Warning Systems.* GSMA.

Sirnate, V. and Jain G. (3 April 2023). "Democracy is dying in digital darkness." APC.

Slim, H. (2022). *Solferino 21: Warfare, Civilians and Humanitarians in the 21st Century.*

Tindall, T. (1 February 2022). "Blackout: understanding the internet shutdowns in Kazakhstan and Yemen". ODI.

UNHCR. (2016). *Connecting Refugees.*

UNHCR. (2023). *Digital Transformation Strategy 2022–2026: Strengthening protection, building self-reliance and optimizing delivery.*

UNHCR. (2023). *Refugee Data Finder.*

Vincent, J. (19 January 2022). "A lone undersea cable connected Tonga to the world – a volcanic eruption broke it". *The Verge.*

World Bank and GSMA. (2020). *The Welfare Effects of Mobile Broadband Internet:Evidence from Nigeria* (English).

World Bank. (2023) *Digital Hotspots: Developing Digital Economies in a Context of Fragility, Conflict and Violence.* Washington, DC.

GSMA Head Office
1 Angel Lane
London, U.K.
EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600