HOLDING SPACE FOR HUMAN RIGHTS: IMPROVING THE GOVERNANCE OF SATELLITE INTERNET CONNECTIVITY

accessnow

accessnow.org

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

HOLDING SPACE FOR HUMAN RIGHTS: IMPROVING THE GOVERNANCE OF SATELLITE INTERNET CONNECTIVITY

Acknowledgements
This report is an Access Now publication, written by Felicia Anthonio, Peter Micek, Giulio Coppi, and Yichen Liang. The authors would like to thank the Access Now team members who provided support, including Kassem Mnejja, Marwa Fatafta, Méabh Maguire, Naro Omo-Osagie, Loren Giordano, Raman Jit Singh Chima, and Zach Rosson.

For more information, please visit:
https://www.accessnow.org

Published in February 2025

Table of contents

Connecting the unconnected: status update

Humans look upward when they need hope. The sky holds enough space to test our big ideas and ample room for dreams to expand. In the digital age, disconnected communities also look up in the hope of realizing the as-yet unachieved promise of connectivity for all.

Despite having laid cables under the sea and ground, and erected towers in jungles, deserts, and cities, at least 2.6 billion people worldwide are still unable to access high-quality, open, secure internet, decades after its invention. And even though mobile phones are now nearly ubiquitous, the growth rate of mobile connectivity has actually slowed in recent years. Such digital divides harm groups experiencing vulnerability or disadvantage, young women and girls in low- and middle-income countries in particular.

Contrary to popular belief, the "digital divides" are not merely the result of geographical or economic conditions, but rather emerges from several, intersecting forms of repression across political, ideological, religious, ethical, and patriarchal lines. We therefore prefer to speak of multiple intersecting "digital divides" that are rooted in discrimination, rather than natural forces.

Even where the promise of stable and accessible internet has been fulfilled, it has proven to be fragile, subject to the whims of authoritarian governments, heavy-handed regulators, or brutal warring actors. Across the world, expanded access to connectivity and devices does not prevent the number of internet shutdowns from increasing year after year. In 2023, the #KeepItOn coalition documented the highest-ever number of recorded shutdowns, with authorities in 39 countries imposing at least 283 shutdowns during conflicts, protests, exams, elections, and more.

Digital divides only widen during shutdowns and communication blackouts. Shutdowns often deliberately target marginalized populations like ethnic minorities, LGBTQ+ communities, and people under military occupation. They are often implemented in targeted local areas and for mobile internet only, making it even more difficult for communities with unstable and nascent internet access to remain connected.

Each shutdown reinforces the need for internet freedom defenders to champion alternatives for bringing people back online. Communities and their advocates benefit from extensive experience in testing and deploying innovative alternatives to missing or insufficient connectivity systems, even in remote or restricted areas, but none have yet proved to be a silver bullet in situations of crisis.

Identifying an appropriate emergency connectivity system requires trial and error, making the process risky, slow, and far from scalable. While one solution might work in one area, it may not be effective a few hundred kilometers away. For example, mesh networks offer resilience and scalability, but

demand a minimum technical capacity and a stable power supply. Combining multiple internet connections in bonded routers, on the other hand, increases reliability and speed, but requires stable cellular networks and generates high costs. Other alternatives exist, but all come with a complex set of trade-offs and requirements. Financing these initiatives requires dedicated efforts and often faces frustrating intransigence. Unfortunately, the best system to use during a crisis is one tested and trusted before the crisis hits, by those who invest in freedom of expression before and after conflicts, and prepare well ahead of particular moments of risk.

As state and non-state actors' cyber operations disrupt essential services, digital governance infrastructure, and economies, the constant increase in the frequency, intensity, and number of shutdowns is having an indiscriminate, disproportionate, and excessive humanitarian impact. But shutdowns can also do more incisive damage. Armed actors increasingly restrict connectivity and use digital communication tools to accelerate and extend the reach and scale of information operations that fuel violence in breach of international humanitarian law (IHL), well beyond the usually acceptable limits of war-time propaganda.

With civilians left in the dark, humanitarian access obstructed both physically and digitally, cyberattacks targeting essential services, and the increased use of harmful information and weaponization of personal digital devices, connectivity is an issue that carries multiple layers of harms — one that we are only just starting to unpack.

Innovating connectivity: harder done than said

In the past decade, traditional terrestrial technologies have struggled to expand broadband coverage to many remote and restricted areas. Some companies have sought alternatives in the form of satellite or aerial internet systems, but to date, most of these have failed to scale.

Satellite connectivity solutions are not new. Geostationary satellites (GEOs), which beam connectivity from their high orbits back down toward the Earth, have been around since the 1970s, and some specific networks, such as the Iridium constellation (brought to popular attention in Hollywood blockbuster film *World War Z*, among others) have been functioning since 1998. The word "geostationary" means that these satellites rotate with the Earth, always serving users across the same broad geographical area. This provides stability and reliability to the connection line, but the data transfer delays, or "latency" (usually insignificant for most personal or professional uses), caused by the distance make the approach sub-optimal for critical systems requiring almost real-time command and control.

Services such as FreedomSat, Thuraya, SES, Cisco, and others cater to humanitarian organizations working in disaster recovery or extreme environments, but even their most innovative approaches have thus far failed to bring down access barriers for small organizations and local communities. Even when costs have been lowered by Viasat and HughesNet, their complexity and higher latency make them difficult to deploy for locally-led emergency response.

Grassroots organizations, Indigenous groups, small companies such as DeFuTech, international or intergovernmental organizations like UNHCR and the International Telecommunication Union (ITU), and NGOs like Telecoms Sans Frontieres have developed effective systems. These sometimes work with local communities, UN agencies, or governments to deploy quickly in remote locations. But their effectiveness is hampered by bureaucratic, logistical, and financial hurdles imposed by authorities or armed groups, by a lack of flexible and agile funding, and by their dependency on an access point to quality internet, be it through fiber, copper, Global System for Mobile Communications (GSM), or satellite.

Among private actors, a range of billionaires, startups, and Big Tech companies continually propose, pilot, and abandon projects to beam the internet from the skies. Facebook's drone-based-internet program Aquila launched to great fanfare in 2014, only to end with a whimper in 2018. A similar fate hit Google-owned company X's Project Loon, which started in 2011, but was discontinued just a few years later.

No advocate for free, open, and secure internet connectivity would celebrate the demise of ambitious moonshot internet projects. Too many communities have no internet coverage, or must pay high fees for low-quality connectivity. Many rural communities already depend on overly expensive satellite connections, while many legacy telecom providers enjoy monopolies and high profit margins, with little incentive to expand services or make room for new market entrants. We need big, new ideas implemented by local communities in a rights-respecting way.

What are LEOs and how do they differ?

The space connectivity industry's traditional actors, such as the GEO companies mentioned above, are no longer the only main player in the space connectivity field. A host of businesses are developing a new form of satellite communications, largely using relatively lightweight, low-Earth-orbit (LEO) constellations. These new LEO constellations, which link hundreds or thousands of satellites in an enormous laser mesh network, intend to reduce latency by reducing the distance that a data signal has to cover when in transit.

The LEO satellites' constant orbiting around the Earth means they will temporarily pass over all countries, including those with less lucrative markets or lacking adequate telecommunications infrastructure. However, the reduction in price, albeit significant when compared to existing options, has not yet proven enough to make LEO internet connectivity easily accessible for most households in poor and disconnected areas. Proponents of the LEO approach claim that, as companies gain traction and customers, they will be able to substantially reduce their pricing, with more established markets covering the entire system's running costs and ensuring enough profits to cover subsidies for lower income markets.

Several companies, including Starlink (SpaceX), Project Kuiper (Amazon), OneWeb (Eutelsat), Telesat Lightspeed, and AST SpaceMobile, are currently competing to launch thousands of these satellites, with Starlink having gained a solid lead in this new space race. In the 1990s, many low-earth-orbit (LEO) satellite internet providers struggled to meet their global ambitions and "impressive plans,"and went bankrupt, like OneWeb, which already failed at least once before returning to the competition in the last few years. But technical breakthroughs have allowed companies to improve their performances and sustainability over time, resulting in the more positive recent trend.

Given that the mission-critical functions most likely to benefit from LEOs are often related to core public infrastructure, defense, or emergency response systems, governments are also backing some of these ventures. For example, China's Qianfan has begun launching LEO satellites with funding from Shanghai's municipal authority. Meanwhile, Starlink receives U.S. government funding through SpaceX contracts, in what has quickly transformed from a solidarity investment to a defense one. Having feebly claimed that their system was only supposed to be used for humanitarian and civilian purposes, Starlink then launched a defense vertical for its business, "Starshield," which formalizes the ever-growing military uses of their terminals by both sides of the conflict in Ukraine and in other areas such as Sudan.

What transpires is a very delicate balancing exercise whereby the digital rights unlocked by new forms of satellite internet connectivity may come with worrying trade-offs in terms of privacy, data protection, information integrity, and dependency on a single provider. Satellite services may help overcome challenges such as keeping the network active even in case of localized technical issues. For example, as it stands, damage to a single undersea cable can cut a whole region's connectivity, while LEOs open up the possibility of rerouting the signal in case one or more satellites fail.

While new forms of space connectivity are slowly becoming available to those with the means and possibility to afford them, we doubt that the companies or their new products will fundamentally change the current inequitable conditions. And without proper human rights frameworks and progressive governance models, they also open up a new set of risks.

It seems clear that what we deserve, and what is overdue, is a solid, human rights-based approach to ensure that emerging and future forms of connectivity respond to everyone's needs in an open, safe, and fair manner. This also demands that authorities come together to develop a new, intentional, digital public infrastructure governance model that is up to the challenge of regulating and overseeing satellite internet infrastructure companies.

Can LEOs help fight internet shutdowns?

Whenever the internet is shut down, people struggle to connect with the rest of the world. We have seen people and communities turn their hopes to the sky as the existing internet system based on fiber cables and towers slowly falls into disrepair, and in order to bypass mandated shutdowns in Sudan and Myanmar, among others.

Time and time again, legacy GEO internet providers have proven the true global coverage and the resilience of their services. Unfortunately, they also hit a capacity and cost roof a long time ago, with their services mostly supporting wealthier military, public, humanitarian, or commercial actors. On the other hand, LEOs show potential for covering remote and hard-to-reach areas, even on the move, and at a much lower cost.

At the time of writing however, all of them, with the exception of Starlink, appear to be struggling to deliver on their business plans, and none seem to be inspired by human rights, led by marginalized communities' needs, or governed in alignment with those communities' priorities.

Despite the rough start, satellite connectivity is increasingly playing a vital role in bringing disconnected people back online by mostly operating in a regulatory vacuum, and it has been tolerated by authorities dealing with crises, to help deliver humanitarian aid and emergency services sometimes even during conflicts.

However, it remains to be proven whether it would help during key national events such as protests and elections, when authorities intentionally shut down the internet with the aim of silencing people and controlling information flows. When governments deliberately shut down the internet, they also adopt measures to counter any circumvention techniques, which could include alternative connections such as satellite.

What does it mean for human rights?

Corporate capture

The advantages seem evident. In an open, diverse, well-regulated market, adding direct satellite connectivity to the existing telecommunications technology stack would likely result in increased opportunities for everyone. Previously unconnected communities might benefit from good quality internet and cellular connectivity, without having to wait for investment in and installation of costly infrastructure such as towers and fiber-optic systems.

The true potential of open connectivity, however, will only be fulfilled by building on existing networks, instead of reducing them to a satellite-only option. An all-inclusive approach encompassing diverse, safe, open, accessible, and decentralized networks, using a variety of technologies, would allow people and local organizations to enjoy previously inaccessible socio-economic and cultural rights. Self-governance of telecommunications infrastructure facilitates community autonomy — even in the face of patriarchal restrictions — and sustainability. It would improve crisis preparedness, early warning, and monitoring; increase disaster resilience; and open up new and lasting post-crisis solutions.

In contrast, making entire population segments dependent on satellite internet could expose underserved communities and regions to the whims of the market or a single company's management decisions. Changing financial or political winds could see providers cease service provision in certain countries or populations, or unilaterally change pricing, terms and conditions. This is especially true for privately-held companies such as Starlink, that are prone to extractive practices in host countries.

At the very minimum, it is warranted to question which consequences would arise from fully entrusting one or two corporate actors with the possibility of launching ever-growing swarms of globally strategic space assets, which may imperil other satellites providing essential services, alter the course of military operations on a whim, lack even the minimum pretension of social and human rights corporate responsibility, and most importantly, fail to serve the unconnected when they are the most vulnerable.

Surveillance and geolocation

Abusive surveillance can happen on all communication systems, and satellite is no different. Just as mobile companies and telecommunication providers can pinpoint or triangulate the position of devices connecting to their network and potentially intercept their signals, satellite internet services know the location and the bandwidth usage of those transmitting from Earth and back.

Encryption still matters. In the case of LEOs, it is unclear to what extent providers will be able to access transmitted content itself, but no company has shared any plans to allow independent audits of their data transmission's encryption system. This concern is all the more relevant given that, at the time of writing, Elon Musk, CEO of Starlink —a company alleged to know more about remote areas of some countries than the local governments — is actively influencing U.S. government policies and meddling with electoral processes inside and outside of the U.S.

Transferring data to and from a satellite also presents another inconvenience, as the source of the signal on the ground (the communication device or terminal) can be very precisely identified and tracked. In situations of conflict or violence, this may represent an additional risk for civilians using the same system as a warring party, as they could be misidentified and wrongly targeted. Similarly, the use of satellite terminals could immediately give away the exact location of any group trying to hide from persecution.

Many existing satellite services only serve major, household name telecom operators. As individual consumers, we may not directly engage with the satellite operators, who serve the airplanes, towers, ships, or any other private and public spaces whose wireless internet we're using. However, as it becomes more common for satellite internet services to directly serve individuals, some of the potential for circumvention and bypassing censorship may be stifled by governments expanding existing license or access requirements to operate in a jurisdiction, including their ability to intercept networks.

This could increase the risk of surveillance, especially if authorities mandate that users register with some form of ID in order to use the service in question, or that providers hand over data without demanding a due legal process.

Finally, some companies' ongoing efforts toward vertical integration, whereby the internet provider owns all connections, hardware routing, and delivery service, could expose people to unlawful privacy violations by operators themselves.

Net neutrality

When internet access depends on just one or two providers, the risk of net neutrality violations grows. The concept of net neutrality ensures that people can access any lawful internet services and data without discrimination, and it requires regulation to ensure that operators do not collude or charge more based on the size or type of content transmitted, nor who sends or receives it.

Reliance on just a few global operators could result in unfair access conditions through tiered pricing discrimination, anti-competitive traffic management practices, and favored status for select content providers, especially in places where national regulations do not explicitly mandate or protect net neutrality. The LEO industry's monopolistic approach risks only benefiting those already able to afford

broadband internet access, in a way that prizes individualism and magnifies global economic inequalities. As Steve Song points out, this comes at the expense of more sustainable, community-led solutions.

Humanitarian neutrality

In addition to net neutrality, humanitarian neutrality might also be affected by reliance on and use of increasingly militarized networks and systems. Humanitarians have historically used either various unsecure civilian telecommunications when still available, or secure independent satellite networks through GEOs when able to afford it.

The advent of LEOs offering military, civilian, and relief services on the same platform could imperil local humanitarian actors' safety. Relying on a retail provider such as Starlink, because GEO services are either unaffordable or less flexible, could make local humanitarian actors harder to distinguish from military or paramilitary groups using the same network. This could result in misidentification and targeting by armed actors, or could even sow doubt as to aid groups' neutrality, exposing them to deliberate attacks.

Weaponization of space systems

Similar doubts could be cast on satellite networks themselves, meaning that any increased resilience introduced by space-hosted hardware would prove to be short-lived, as geopolitical powers develop space countermeasures. Just as cellular towers and data centers are targeted in today's conflicts, there is no reason to believe that the same will not happen to space capabilities and operators, as happened at the beginning of Russia's full-scale invasion of Ukraine, if they are seen as directly participating in hostilities. This scenario warranted a special mention in the EU's recent Space Strategy for Security and Defence, which warned of "an arms race in outer space" and of space "becoming an area of conflict."

Overall, it seems unlikely that communities could rely on satellite systems' geopolitical independence , given their presence and coverage is driven by considerations other than local communities' needs.

National governments are still grasping to control these global services. Iran convinced an ITU board to mandate that the U.S. and Norway take "immediate action to disable Starlink terminals" and cease its operations in the country, leading Starlink to delete Iranian user accounts. In addition to applying diplomatic pressure in multilateral institutions, Russia seeks to obstruct access to satellite internet through technical blocks using strategic military and tactical means. France has introduced a Law on Space Operations that allows the government — under specific circumstances — to seize any private space asset and put it under military control. Some governments or armed actors might choose to prioritize service delivery to certain areas over others, based on allegiances, corruption, or loyalty,

while preventing foreign operators from deploying their services because of conflicting geopolitical interests (e.g. Yemen, Sudan), suspicions about hidden agendas, or simply because they want to maintain control over internet connectivity (e.g. Cuba).

Environmental and safety risks

The growing presence of LEO hardware carries significant environmental risks. It is estimated that there are close to 6,500 Starlink satellites in orbit, and possibly 1,000 belonging to their main competitor, OneWeb, while Amazon aims to launch at least 3,000 in the next few years. Some estimates suggest there could be as many as 100,000 satellites in orbit by 2030.

This surge in satellites will force the ITU to impose more stringent regulations, as the number of LEOs is growing so fast that there may soon be no room for new satellite deployments. Critics have flagged how public funds are being used to create space junk that is polluting our night skies, while the radio and light pollution generated by so many systems in such a relatively limited space is already having an environmental impact — and as their number increases, so does the risk of collision and creation of dangerous debris. Space debris often burns up by falling into the Earth's atmosphere. However, debris that remains floating in orbit can render the area unusable or too dangerous for a very long time, and additional debris formed by each collision further saturates an already crowded environment. In August 2024, a rocket carrying China's Qianfan satellites broke up upon launch, creating more than 700 pieces of debris.

If systems aren't equipped with adequate steering, propulsion or other collision-avoiding systems, the consequences could be catastrophic. Floating debris could trigger a cascading sequence of impacts transforming an environmental risk into a physical one that "render[s] near space unusable," a phenomenon known as the Kessler Syndrome.

Given the global nature of LEO orbits, worldwide coordination on governance is necessary. Multiple jurisdictions, such as the U.S. and Germany, have devoted regulatory efforts to mitigate orbital debris, and in 2023, the European Space Agency (ESA) launched its "Zero Debris Charter," an internal standard aimed at significantly reducing the generation of space debris in both Earth and Lunar orbits by 2030 — the first ambitious goal of its kind.

At the UN, the ITU currently coordinates satellite trajectories to prevent collisions, and is working to address new LEO technologies. As part of its efforts, the 2022 ITU Plenipotentiary Conference revised Resolution 186 to establish an enhanced framework for international monitoring between the ITU Radiocommunication Bureau, national administrations, and designated satellite monitoring facilities.

Global cooperation and regulation are essential. Any collision in space could be catastrophic, and satellite constellations must coordinate their routes. There are usable corollaries in the Outer Space Treaty, and historical precedent in the law of the seas. As one participant in a 2020 workshop organized by Access Now noted, "We pulled it off on the high seas, and should be able to pull it off here as well."

Gaps in regulation and global governance

Despite satellite connectivity's significant role in advancing global telecommunications, existing legal frameworks and even non-binding agreements have yet to address its human rights implications. International law, focusing on international cooperation, peaceful use of space, registration, and liability attribution, largely overlooks the intersection of satellite communications with fundamental human rights such as access to information, data privacy, and freedom of expression. Given growing digital divides and potential surveillance concerns, such a legislative gap must be examined and addressed.

National and regional satellite regulations are rapidly evolving, generally prioritizing national security, economic growth, and technological sovereignty (e.g. EU, Germany), rather than human rights considerations. States seem more concerned with operational, technical, and strategic goals than the societal impacts of satellite communication activities on human rights.

As already mentioned, some states have recently incorporated sustainability concerns into their national space laws. However, a comprehensive and inclusive governance framework addressing critical human rights and humanitarian issues in satellite connectivity is yet to be developed. Using spaces open to us, like the UN Internet Governance Forum (IGF), Access Now has repeatedly convened satellite experts and impacted communities.

Unfortunately, the ITU, which plays an established role in satellite governance, remains largely inaccessible to civil society, as do the secretive national defense and security agencies that fund many space initiatives.

There is an urgent need to develop more open governance bodies and targeted regulations that explicitly integrate human rights protection measures, to ensure that satellite connectivity serves as a tool for inclusion and empowerment, rather than exacerbating inequality and insecurity or infringing freedoms. These processes must also welcome diverse stakeholders by design; those communities left behind by decades of telecommunications development deserve first place in any satellite internet governance bodies. What we do on Earth today will not only determine whether we reach existing goals such as the 2030 Agenda, but could also shape the path for the interplanetary internet of tomorrow.

Conclusions and recommendations

Overall, we welcome the expansion of opportunities for connectivity that, for once, appear to serve remote and underserved communities by design, rather than as an afterthought. Small island developing states, Indigenous communities, and isolated groups all look to satellite services with hope. We believe that a holistic approach to connectivity, which treats it as a shared resource across sea, land, air, and space, would allow all humanity to benefit from open, safe, and fair internet access.

However, we are also concerned that civil society groups sounding the alarm about corporate control over such an essential resource are being ignored. Market, financial, and military interests are driving what should be managed under a common, rights-respecting governance protocol. So far, the promise of global connectivity is held in the clutches of just a few Big Tech companies, all in a "space race" with each other that has few rules and even fewer accountability mechanisms.

Not only is the global governance framework lacking, but so are basic corporate policies. Strong and auditable encryption, data minimization, and human rights due diligence are needed to prevent greater centralization, the abuse of personal data, and the normalization of surveillance practices. Net neutrality and privacy-by-design policies should be required. Without these safeguards, a handful of powerful service providers may recreate many of the existing inequities and risks of social media and internet infrastructure platforms, with even more centralized monitoring and control capabilities. Regulations must be co-created, enforced, and adapted where appropriate.

In the meantime, national regulations and intergovernmental entities' guidelines might provide some control over these companies, reining in some of the advantages that made these technologies attractive in the first place. Rather than striking deals directly with end users, satellite companies will likely be requested to lease space to internet service providers or telecom companies in each of the countries that the satellites pass over.

This could recreate the current tension between allowing Big Tech companies to pick and choose the laws and norms they respect, and giving states having unchecked power to disconnect communities within their jurisdiction. Spectrum allocations like those of ITU-R may come into play here, in addition to any domestic telecommunications laws and regulations applicable to satellite frequency bands.

Conceiving of space as a commons and of the networked systems powering the internet as part of a global digital public infrastructure is incompatible with the current for-profit approach. Greater UN and multi-stakeholder cooperation will be needed to navigate the many economic, environmental, political, policy, and human rights impacts and interests at play. We have driven conversations on satellite internet governance at fora such as RightsCon and global IGF meetings, inviting satellite

providers and regulators to participate, but our outreach efforts have not been reciprocated. Civil society still has no dedicated seat at the satellite internet table.

Our recommendations

We hereby call on states to:

- Put human rights at the heart of connectivity governance, encompassing satellite and space internet services, by developing more detailed policies and rules that explicitly center inclusion, accessibility, and co-creation, and integrating human rights and non-discrimination to ensure that emerging connectivity systems serve as an equitable, rights-respecting tool for sustainable development;
- Reaffirm and strengthen humanitarian protection measures for connectivity to prevent the weaponization, abuse, targeting, and destruction of civilian and emergency telecommunication infrastructure across sea, land, air, and space;
- Build capacity through educational programs, forums, and regulatory initiatives on satellite internet services, funding robust participation that enables marginalized and vulnerable communities to assert their rights to privacy, freedom of expression, and non-discrimination, and to engage in relevant policy development and enforcement;
- Ensure coherence between humanitarian and human rights law and policy, by reaffirming international legal protections for civilian internet connectivity and related infrastructure, and by setting up adequate deconfliction mechanisms to ensure the continuity of life-saving telecommunication activities during crises or emergencies;
- Introduce or strengthen regulations and policies ensuring adequate independence, competition, and diversity in connectivity services, provide adequate legal and judicial guarantees protecting all telecommunication services and providers in the lawful exercise of their activities without interference, and establish restrictions, transparency, recourse, and accountability mechanisms for any process that might obstruct community access to these services; and
- Strengthen access-promoting measures such as the universal service funds, in order to expand internet access to historically marginalized communities in particular, and explore potential equitable subsidies for satellite internet services.

We call on all armed parties to:

- Recognize civilian connectivity infrastructure's protected status, and refrain from weaponizing or targeting any part of it in an effort to punish or terrorize local communities;
- Commit to protecting and promoting access to telecommunications and internet connectivity for affected populations in times of crisis or conflict, including during negotiations for ceasefire and peace agreements; and

- Respect and facilitate all actors' work to set up, maintain, and repair civilian internet connectivity, including community and Indigenous-led networks.

We call on the ITU and its working parties to:

- Prioritize human rights and humanitarian considerations when developing guidance and policies on LEO connectivity systems, and adopt a rights-based approach to their analysis and recommendations; and
- Take a multi-stakeholder approach to defining governance and technical standards for the future of internet connectivity, and be more transparent and open when communicating about current and future processes.

We call on satellite and internet companies to:

- Adopt and implement new policies respecting human rights and humanitarian principles, building on existing relevant frameworks, including the *UN Guiding Principles on Business and Human Rights*, *OECD Guidelines for Multinational Enterprises*, and *Geneva Conventions*.
- Be transparent and consistent about the policies and procedures guiding decisions related to partnerships and procurement with states and local providers;
- Invest in human rights due diligence to develop and maintain policies and protocols on rights-preserving issues such as encryption, lawful intercept, human rights monitoring, data protection, and net neutrality, while reaffirming the refusal to engage or support unlawful or unethical practices such as unlawful surveillance and censorship;
- Adapt policies and practices for situations of crisis, including disaster response and conflict, in close coordination with affected communities; and
- Establish and maintain regular and open channels for aid and human rights actors to communicate on current, emerging, or potential issues and threats to connectivity networks and their users, in a timely and effective manner.

We call on the humanitarian community, and notably the Red Cross and Red Crescent movement, the Emergency Telecommunication Cluster, the UN agencies, NGOs and their public and private partners to:

- Prioritize emergency connectivity for affected communities and humanitarian responders, and plan for resilient and multilayered connectivity stacks within crisis preparedness and prevention strategies; and
- Include standards on civilian connectivity and communication systems in any existing and future operational guidance on protection strategy and activities.

For more information:
Giulio Coppi (giulio@accessnow.org)

Access Now (https://www.accessnow.org) defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.